Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2013-03

Measuring Security Effectiveness and Efficiency at U.S. Commercial Airports

Diehl, Daniel

Monterey California. Naval Postgraduate School

http://hdl.handle.net/10945/32812

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MEASURING SECURITY EFFECTIVENESS AND EFFICIENCY AT U.S. COMMERCIAL AIRPORTS

by

Daniel Diehl

March 2013

Thesis Advisor: James Wirtz
Second Reader: Christopher Bellavita

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE MEASURING SECURITY EFFECTIVENESS AND EFFICIENCY AT U.S. COMMERCIAL AIRPORTS		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Daniel Diehl			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Civil aviation contributes over $900 billion to the U.S. economy annually and the cost of securing U.S. aviation against criminal and terrorist attack runs in the billions of dollars. Therefore, it is critical to use appropriate metrics in managing the security policy and programs. Nonetheless, aviation security has typically evolved haphazardly as a reaction to changing criminal events, often resulting in widespread controversy. The U.S. Government Accountability Office and the media have questioned many Transportation Security Administration procedures. This thesis uses formative program evaluation and policy analysis to investigate current assessment of airport security programs. It identifies innovative public administration and policy-analysis tools that could provide potential benefit to airport security. These tools will complement the System Based Risk Management framework if the Transportation Security Administration involves more stakeholders in collecting and analyzing pertinent data, proactive planning, and developing solutions.

14. SUBJECT TERMS Aviation Security, Performance Measurement, Security Metrics, Public Administration, Commercial Airports, Security Strategy, Homeland Security			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MEASURING SECURITY EFFECTIVENESS AND EFFICIENCY AT U.S. COMMERCIAL AIRPORTS

Daniel Diehl
Battalion Chief, Atlanta Fire Rescue Department (Retired),
Fire Science Coordinator, Atlanta Technical College
B.S., Covenant College, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2013**

Author: Daniel Diehl

Approved by: James Wirtz
Thesis Advisor

Christopher Bellavita
Second Reader

Harold A. Trinkunas, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Civil aviation contributes over $900 billion to the U.S. economy annually and the cost of securing U.S. aviation against criminal and terrorist attack runs in the billions of dollars. Therefore, it is critical to use appropriate metrics in managing the security policy and programs. Nonetheless, aviation security has typically evolved haphazardly as a reaction to changing criminal events, often resulting in widespread controversy. The U.S. Government Accountability Office and the media have questioned many Transportation Security Administration procedures. This thesis uses formative program evaluation and policy analysis to investigate current assessment of airport security programs. It identifies innovative public administration and policy-analysis tools that could provide potential benefit to airport security. These tools will complement the System Based Risk Management framework if the Transportation Security Administration involves more stakeholders in collecting and analyzing pertinent data, proactive planning, and developing solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....1
B. RESEARCH QUESTION....5
1. Primary Research Question....6
2. Secondary Research Questions....6
C. ARGUMENT....6

II. LITERATURE REVIEW....13
A. HISTORIC/TECHNICAL TEXT AND ARTICLES....13
B. GOVERNMENT DIRECTIVES AND POLICY....15
C. CONGRESSIONAL REPORTS....19
D. PUBLIC ADMINISTRATION AND PERFORMANCE MEASUREMENT....21
E. ACADEMIC RESEARCH....22
F. FIRE PREVENTION LITERATURE....24
G. CONCLUSION....27

III. METHODOLOGY....29
A. OVERVIEW....29
B. SURVEY....29
1. Round One Survey Questions....29
2. Round Two Survey Questions....30
C. LIMITS OF THE EMPLOYED METHODOLOGY....30
D. PROPOSED RECOMMENDATION....31

IV. ANALYSIS/FINDINGS....33
A. ANALYSIS INTRODUCTION....33
1. First Round Survey....33
2. Second Round Survey....39
B. FINDINGS....43

V. CONCLUSIONS....47

APPENDIX....53
A. DELPHI SURVEY ROUND ONE....53
B. DELPHI SURVEY ROUND TWO....59

LIST OF REFERENCES....63

INITIAL DISTRIBUTION LIST....71

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Table of Aviation Crime and Fatalities....2
Figure 2. Chart of Aviation Crime and Fatalities....2
Figure 3. System-Based Risk Management Process (From: Department of Homeland Security 2007)....17
Figure 4. Supporting Plans to the National Strategy for Aviation Security....19
Figure 5. U-Map Sunburst Charts....24
Figure 6. Fire Safety Concepts Tree....27
Figure 7. What Criteria Do You Currently Use to Judge the Efficiency and Effectiveness of Airport Security Policies and Programs?....34
Figure 8. Which of These Do You Consider Most Useful and Why?....36
Figure 9. What Metrics … Would You Like to See Employed?....37
Figure 10. Why a Secure Web-Based, Professional Network, Dedicated to Airport Security Information Sharing, Would Be Feasible and Worth the Effort?....40
Figure 11. Is the International Civil Aviation Organization Security Audit Program a Valuable Tool?....41
Figure 12. What Methods Would Best Help Determine How to Allocate Security Resources?....43

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. International City Management Association Suggestions for Measuring Effectivness.....11
Table 2. How to Analyze a Security System 15
Table 3. Suggested Congressional Investigations.....21
Table 4. Steps to Design a Fire Safety Program (From: Rasbash et al., 2004).....26

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, to my wife, Sharon, for all the weeks she held down the fort at home while I was in residence at Monterey and for every time I said I could not do something because I had to work on this thesis.

To my parents, Warren and Virginia Diehl, for their support through every phase of my career and education.

To the Atlanta Fire Rescue Department and the City of Atlanta, for allowing me to attend The Center for Homeland Defense and Security.

To my theses advisor, Jim Wirtz, and second reader, Chris Bellavita, for taking interest in my research before I did and providing much needed guidance at each critical juncture. They truly made this thesis possible.

To Cohort 07–11 (CA0705/0706), for inspiring me to dig deeper and think harder, I will never be the same. Although, I struggle to comprehend how I deserved to be part of that amazing group of public service professionals, I must trust in Divine providence.

Finally, and mostly, to my sister Debby, whose prayers and faith kept me going.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> Either actual war, or constant studious preparation for war, actually never ceases. And it is difficult to say which is the worse of the two…The never-ceasing preparation for war seems actually to cost more. (Gordon, 1914)

A. PROBLEM STATEMENT

Since the late 1960s, the United States (U.S.) government has reacted to aviation crime by hastily implementing new regulations, often without the benefit of structured analysis. On September 11, 2001, al Qaeda increased the stakes in the effort to guarantee airline passenger safety. As a result, the United States ramped up its counter tactics. Numerous studies describe how when the programs mandated by these new regulations are evaluated, the lack of specific objectives, goals, and accepted standard measurements, prevent reliable conclusions. With today's public sector deficits and thin airline profit margins, airport operators and regulators need a dependable system to gauge the effectiveness and efficiency of airport security.

Aviation security has evolved reactively, transforming as criminal tactics changed. Prior to 1948, incidents of aeronautic malevolence were a nonissue and averaged less than one per annum (See Figures 1 and 2). From 1948 to 1968, skyjacking became a common mode to attempt to escape communism. However, these attempts normally ended with the perpetrator being shot or arrested and since the United States supported these defections, increased security was considered cost prohibitive.

Decade	Domestic Events	Domestic Fatalities	Global Events	Global Fatalities
1940s	0	0	7	25
1950s	2	45	13	21
1960s	6	136	9	244
1970s	2	0	21	559
1980s	3	314	12	869
1990s	0	0	4	37
2001+	1	0*	2	90

* Does not include the 2532 deaths during 9/11.

Figure 1. Table of Aviation Crime and Fatalities

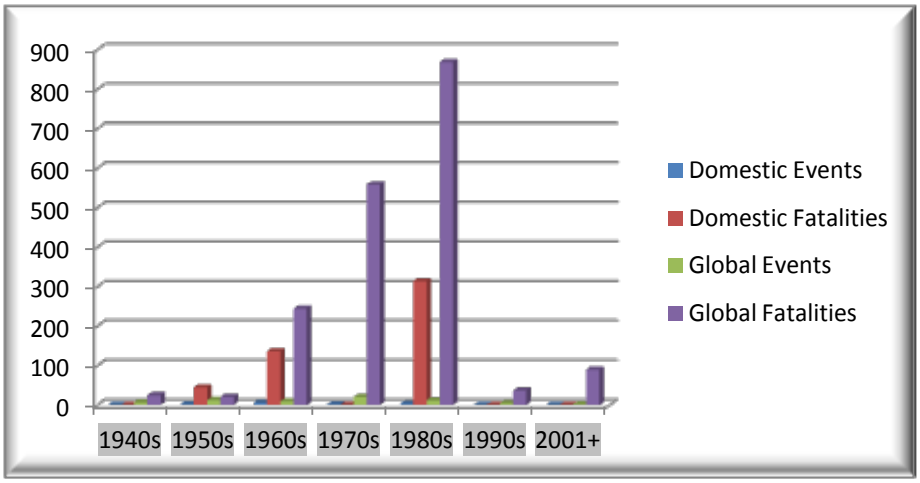

Figure 2. Chart of Aviation Crime and Fatalities

In 1944, the International Civil Aviation Organization was formed and met in Chicago to "secure international cooperation" in establishing standards and procedures to advance civil aviation and has been a major factor in aviation security. Today, the organization is an agency within the United Nations with 188 nation members. The majority of airport security policies throughout the world are based on The International Civil Aviation Organization Annex 17, Standards and Recommended Practices, and security manual. The Aviation Security Plan of Action includes a Universal Security Audit Program based on Annex 17 standards. Although each program must be passed by a majority vote of all member states, none of these guidelines is compulsory until adopted

by local jurisdictions. Generally, the U.S. Transportation Security Administration requires international airports to adopt International Civil Aviation Organization security standards before allowing U.S. carrier service, and U.S. aviation regulations generally exceed these standards (Price & Forrest, 2009, pp. 85–91).

In 1968, the Popular Front for the Liberation of Palestine changed the game by holding Israeli El Al Flight 426 hostage for five weeks. Israel set a risky precedent by releasing 16 convicted Arab prisoners to end the standoff (Thomas, 2008; World: Drama of the Desert, 1970). By 1970, in response to dramatically increasing fatalities and capital damage, U.S. President Richard Nixon ordered air carriers to install "surveillance equipment" in high-risk airports and reinstituted the Federal Air Marshal Program (Peters & Woolley, 1970). In 1972, one hijacking occurred globally every five days, and two per month in the United States (Thomas, 2008). As a result, the Federal Aviation Administration issued emergency rules requiring the screening of all passengers and carry-on baggage. Two years later, police thwarted a plan to fly a DC-9 into the White House and Congress authorized sanctions against any country failing to meet International Civil Aviation Organization security standards. In 1977, William Landes calculated the number of hijackings probably deterred by screening from 1973 to 1976, and estimated the cost of preventing each at approximately $9 million (Landes, 1978).

By the 1980s, further increases in aircraft bombing, hijacking, and violence toward Jewish and American passengers, along with the advent of real time news coverage, pressured authorities to address security threats more aggressively (Price 2009). In 1985, 30 days after a U.S. sailor was executed on board a hijacked aircraft by Shiite Muslims, Congress mandated luggage be matched to passengers on high-risk international flights (Preston, 2005). Eight days after Pan Am 103 blew up over Lockerbie, Scotland, in 1988, security x-rayed or hand screened all checked bags on U.S. carriers from Europe or the Middle East.

Although the incidence of violence in air transportation diminished during the 1990s, the Federal Aviation Administration estimated $3 million was lost each week in airport retail sales due to the restriction of concourse access to ticket holders. After the

first World Trade center bombing and the Oklahoma Federal Building attack in 1993, a 300-foot vehicle free zone around terminals curtailed the primary source of airport revenue as customers parked offsite.

Compared to other incidents of violence against the airline industry, the September 11, 2001 terror attacks against the Pentagon and the World Trade Center had the greatest impact on civil aviation in the United States. Employers released over 140,000 aviation employees as a direct result of the attack. Less than 11 days later, Congress passed the Air Transportation Safety and Stabilization Act of 2001, and authorized $10 billion in federal loan guarantees and $5 billion in grants to air carriers. Furthermore, it limited reparations for each family of the 9/11 victims to $1.6 million. On November 19, 2001, President George W. Bush signed the Aviation and Transportation Security Act of 2001, which altered U.S. aviation security from top to bottom (Cobb & Primo, 2003). The federal government assumed full responsibility for civil aviation security, and transferred jurisdiction from the Federal Aviation Administration to the newly formed Transportation Security Administration, under the Department of Transportation.

As quickly as the government created laws to mitigate new threats to aviation, industry, media, and customers found fault with the plans. In *Beyond Fear*, security guru Bruce Schneier claimed, “with the exception of reinforcing cockpit doors, passengers knowing they have to fight back, and sky marshals…” most aviation security is simply theater. Furthermore, he reasoned terrorists would now target the non-secured side of the security checkpoint (Schneier, 2003).

The U.S. Government Accountability Office has noted that national transportation security standards are not being followed by the airline industry, that inadequate procedures are in place, and that security resources are allocated haphazardly (GAO, 2010b). In 2010, the Government Accountability Office evaluation of how well the Transportation Security Administration (TSA) met National Infrastructure Protection Plan requirements suggested that the agency’s efforts to judge security methods were imprecise and disorganized (GAO, 2009). The Department of Homeland Security Quadrennial Homeland Security Review was designed to help guide policies and

priorities for four years. The Government Accountability Office report on the first review identified stakeholder concerns over the lack of a national risk assessment and that the review was rushed, which further limited the ability of stakeholders to participate in the development and evaluation of metrics related to airline security(GAO Highlights, 2011).

K. Jack Riley, Vice President of the National Security Research Division of the RAND Corporation, is an outspoken critic of national security policy. To quote a recent speech he delivered at the Airport Revenue News Conference, "One reason that we have ended up in the current situation is that security measures are grafted or layered on in response to specific incidents, with little regard to an integrated assessment of cost, effectiveness, and impact on risk" (Riley, 2011). Clearly, an overall assessment of airline security would be a starting point in allocating resources efficiently and in developing estimates of the effectivness of existing security procedures.

Resource allocation and cost assessment are becoming increasingly more important as many airports are owned by states or cities with shrinking budgets. According to the non-profit think tank, Center on Budget and Policy Priorities, "For fiscal year 2013 … 29 states have projected or have addressed shortfalls totaling $47 billion" (Center on Budget and Policy Priorities, 2012). Municipalities are faring no better. In 2009, combined U.S. city budgets were running a three-year deficit that might have been as high as $83 billion (Hoene, 2009). Since 2009, this municipal economic outlook has not improved significantly. In 2011, the International Air Transport Association forecast a 78% drop in the airline industry's profits, which equals a net profit of $4 billion and a profit margin of .07% (Smith, 2011). This results in significant economic incentives to provide a more effective and efficient security system. A structured comprehensive analysis of airline security could help achieve this objective.

B. RESEARCH QUESTION

The purpose of this thesis is to identify and examine concepts and principles used in public administration and fire prevention that could be used to improve the effectiveness and efficiency of airport security policy and programs.

1. Primary Research Question

- To what extent is commercial airport security currently measured and how could it be measured?

To offer a comparative standard to evaluate the results indicated in the primary research question, this thesis attempts to answer the following set of secondary questions.

2. Secondary Research Questions

- What recognized public administration performance metrics are relevant to aviation security?
- Is the international fire safety consensus standard model relevant to aviation security?

C. ARGUMENT

Civil aviation contributes $900 billion to the U.S. economy, or 9% of the gross domestic product (Price & Forrest, 2009). The potential for economic loss and death caused by aviation terrorism has been the justification for billions of dollars expended on aviation security. These figures demonstrate the need for objective, reasonable management of public programs and resources. Competent management is contingent on the application of appropriate metrics. According to Tachi Kiuchi, the Chairman and Chief Executive Officer of Mitsubishi Electric America, "Metrics are to a business what the five senses are to humans - systems of feedback that improve our capacity to adapt and excel over the long run" (Kiuchi, 2002).

Performance measures have been a primary element of many result-oriented management systems. Frederick Taylor is considered one of the pioneers of industrial management because he proposed measuring workload, workflow, and worker efficiency as early as the 1890s. Although, 40 years earlier, the National Board of Fire Underwriters of the United States was formed and applied measures and standards to inaugurate a paradigm shift from accepting risk to managing risk (Brearley, 1916). In 1943, Clarence Ridley and Herbert Simon wrote *Measuring Municipal Activities: A survey of Suggested Criteria for Appraising Administration* for the International City Management Association. At approximately the same time, academia began debating the merits of "specific and measurable" goals or objectives (Morrison, 2010).

Pinkerton Government Services, the security provider for many public facilities, uses an “evaluation tool to document current performance, identify opportunities for improvement, and develop performance enhancement plans” (Maydoney, 2005) at over 100 facilities in the United States. The plan uses percentage points from each evaluation transposed to a master scorecard based on weighted importance. The results are shared with all involved parties including management, supervision, and officers. The plan allows customers a detailed view of performance at all of their locations and answers the question, “Are we meeting your requirements?” (Maydoney, 2005)

Pinkerton is hybrid organization in the sense it is a privately owned corporation but services government facilities, much the same as commercial airports are hybrid, publicly owned for-profit businesses. Therefore, public administration principles combined with performance measurement theory may well provide the tools necessary to ensure that aviation security adapts and improves. Nevertheless, to insure the analysis does not create more trouble or cost than value, the measurement system must be designed, implemented, and supported to serve very specific managerial needs. The litmus test has to be, “Does the organization improve over time?” (Poister, 2003)

Interest in using metrics to judge public programs has also been translated into law. The Government Performance and Results Act of 1993 required all federal agencies to set goals and report annually on performance in an effort to address the absence of information on program outcomes. The Government Performance and Results Modernization Act of 2010 required more frequent reports and defined the performance framework more specifically (Kamensky, 2011). Forty-seven states legislate or mandate per executive order performance-based budgeting along with the necessary performance measures (Poister, 2003). Fire safety has a long history of measuring (and improving) system outcomes, establishing baseline standards, and converting those standards into law. As safety and security share many common objectives, numerous public safety measures and standards may be adaptable to homeland security.

Several factors that determine the consequences of a fire, such as building construction, occupant egress, and human behavior, are equally pertinent to the outcome of a terrorist incident. For example, deflagration is often a significant aspect of both fire and terrorism. Many lessons learned from the post analysis of major fires could be directly applicable to security planning.

Aviation security and fire protection share several objectives and problems in common. The three primary goals of fire protection: life safety, property protection, and continuity of business operations, are inherent in security. Both fields face the challenge of measuring prevention (deterrence), and more specifically, collecting data concerning events that do not occur. The National Fire Protection Association has been involved in such analysis since the dawn of the industrial revolution (Grant, 1996), and as a result, developed a working relationship with the National Institute of Standards and Technology in 1914. Today, the National Institute of Standards and Technology Building and Fire Research Laboratory measures the effectiveness of building and fire codes, structural fire response, occupant behavior and egress, and aircraft impact damage, with some recent research directly related to 9/11 (Diamantes, 2011).

These experiments quantitatively measure the probability of successfully mitigating specific threats with specific strategies. Statistically measuring the quality of service oriented programs like fire safety and security has always been more elusive. The evolution of modern fire service metrics may provide clues to improving performance measurement of aviation security.

The first analysis of fire service performance began in 1916 by the Insurance Services Office, a voluntary, nonprofit association of insurance companies. The grading was and is still a comparative rating of communities' ability to defend against major fires to set insurance rates. It classifies fire protection capability based on staffing, training, equipment, communications, and water supply, and assigns a minimum rating between 1, for excellent capability, and 10, for no fire protection whatever.

In the late 1980s, a fire department self-accreditation process was developed that involved new research and analysis, based on performance measures used in foreign fire services. Early findings indicated U.S. fire departments tracked and reported activity rather than performance, which was of relatively little value in operational improvement or strategic planning (Bruegman, 2012). Although most large fire departments have now made significant progress, many small and volunteer agencies still struggle with implementing meaningful performance metrics. One likely explanation is participation in the national data collection system is not mandatory. However, participating departments, in conjunction with the National Fire Protection Association have developed useful qualitative measures for fire safety programs.

Researchers attempt to quantify risk by assessing the expected incident frequency and the severity of associated consequences. The two primary approaches to quantitative appraisal of fire safety are point schemes calibrated to acceptable standards and mathematical modeling calculating data in estimated ranges, which provide approximated conclusion (Spitzer, 2007). It is easier to address intangibles like “public good” and “political constraints” with statistical metrics, if key value drivers are identified. Performance measurement can be misdirected if not strongly related to mission.

Although defining measure and collecting data are requisite to evaluating programs, the descriptive nature of measures must be differentiated from the appraisal function of a program evaluation (Poister, 2003, p. 12). Data must not be over interpreted. Balancing the number and focus of measures is crucial. Utilizing too many routine measures is a waste of time and resources, while incorporating the most relevant three or four measures can provide important insights into efficiency and effectiveness.

As with all tools, performance measurement systems and data can be deliberately or perfunctorily misused. One common mistake is to prove rather than improve. Therefore, management must periodically assess the entire performance measurement system. Full commitment from management helps assure cooperation and availability of resources. It also is important to secure buy in from all pertinent stakeholders, as those who benefit from current policy or fear new technology may resist the new metrics. In an ideal system, all employees from top to bottom would participate in assessing how well

they meet organizational objectives. Employees already informally measure their own operation and understand how that performance compares with other processes. When employees are empowered to adapt measurements and take necessary corrective action, it minimizes the need for external feedback.

Another measurement error involves confusing output with outcome. Output is the amount and quality of product or service rendered, often related to time or expense (efficiency), while outcome is the degree to which the objective and goals are met (effectiveness). To obtain a complete understanding of service, a measurement system must examine both effectiveness and efficiency. Otherwise, efficiency may be improved while effectiveness slips to an unacceptable level. For example, vehicle inspections may have reached a record unit per staff hour ratio, while decoy explosive devices missed per inspection has increased (Spitzer, 2007). Experience shows that the development of effective measurement is the best way to insure both organizational effectiveness and efficiency (Hatry, Blair, Fisk, Greiner, Hall, & Schaenman, 1992). The International City Management Association offers 10 suggestions for implementing a "system" to monitor effectiveness (Table 1).

Performance measurement can define program service levels, contribute clarity of mission, and communicate program accomplishments to managers, customers, and policymakers. Measures can be used to plan and control programs at the operational level and a strategic level when indicators measure progress toward meeting goals and objectives, and how well strategy translates to action.

Past Government Accountability Office reviews have outlined specific requirements for effective program evaluation, which include performance standards, clearly articulated methodology, and detailed data analysis. All three requirements can be addressed, provided a system is designed, implemented, and supported properly. While it may be challenging to design measurement addressing a particular management question based on the organization's mission statement, articulated goals and objectives, and established standards, it is sometimes possible to extrapolate accepted standards created by recognized industry organizations as a relative measure, e.g., to compare operating costs of different model cars under emergency use and general purpose (Ammons, 2002).

Table 1. International City Management Association Suggestions for Measuring Effectivness

1) Involve individual agencies at all stages of planning and implementation
2) Make the process positive, constructive, rewarding, and unthreatening as possible
3) Provide specific incentives for manager to participate
4) Provide central staff technical leadership and management support.
5) Maximize the utility and application by summarizing the finding concisely and clearly
6) Balance client-oriented outcomes measures and agency-oriented activity
7) Prioritize measuring. Begin with those outputs directly related to customer service
8) Institutionalize measurement activities. Incorporate measures in the budget process
9) Provide in advance for comprehensive discussion of the measures and procedures
10) Find champions, officials must be committed, reexamine procedures after implemented

A performance measurement system generally consists of four components: 1) general management function, 2) data collection, 3) analysis, and 4) consequent action of decision making. Management is responsible for establishing the foundation by clearly communicating the strategic framework. Data collection/processing is often the most resource intense component because raw data has to be processed into statistical values, displayed in useful formats, and compiled in reports after verifying the reliability of the data and processing. The analysis component provides the context or framework and contrasts the data to something to create information and make understanding possible. Usually the primary indicator is performance over time. Nevertheless, other comparisons based on units, agencies, or benchmark performance measures can be constructive. Finally, an effective system is designed to improve performance; the information gained should be the basis of practical decision making and procedural change. All four components should reflect data driving performance.

Performance measurement, however, should be only one consideration in the enhancement process. Further comprehensive evaluations may be justified based on the

results of the analysis. Management must support a performance measurement system over the long term. Evolution via testing on a small scale, revision to meet changing needs, and institution-wide adoption takes time. The temptation to seek a magic bullet measure should be resisted, as measurement is a continuous process of trial, discovery, and innovation, which involves nontraditional concepts (Spitzer, 2007).

II. LITERATURE REVIEW

This review of literature related to aviation security includes historic/technical text and articles, government policy directive-documents and reports, academic research and books, and literature concerning general management, public administration, and performance measurement principles. The main objective is to discover patterns or trends in the writings that will facilitate better understanding of past practices, current applications, and potential future direction of aviation security.

A. HISTORIC/TECHNICAL TEXT AND ARTICLES

Although aviation security has been a policy issue for well over half a century, the study of the topic is relatively new. Overall, technical readings provide a general background of airport security challenges, as well as issues in the planning and implementation of security programs. Some of the writing is critical of administrative policy before and after 9/11, and takes exception to an apparent lack of unity in strategy and execution. Several authors suggest steps to correct some of these perceived deficiencies.

The first edition of the earliest text specifically dedicated to airport security was written in 1976 (Moore, 1991). *Airport, Aircraft, and Airline Security* was a technical instruction text for airport security officers. This book covers the history of skyjacking, terrorism, and the reactive policies of the U.S. and international governments, up through the Aviation Security Improvement Act of 1990. It categorized different options for securing aircraft and airport facilities, including fencing, lighting, employee identification, law enforcement, and contingency planning. The brief final chapter, "Control by Audit and Survey," outlined a self-help security evaluation for airfreight carriers.

Eight years after 9/11, Jeffery Price and Jeffery Forrest released a more up-to-date technical airport security manual for practitioners, *Practical Aviation Security, Practicing and Preventing Future Threats*. It covered more up-to-date national policies and

regulations and included a detailed chapter on 9/11 and the 9/11 Commission Report (Price & Forrest, 2009). Both these books provide an overview of general procedures involved in securing airports against criminal and terrorist activity.

In his book on Aviation Security, Bartholomew Elias, an aviation policy specialist for the Congressional Research Service and a research psychologist for the U.S. Air Force, found fault with four areas in the *National Strategy for Aviation Security*. He believes it does not effectively: 1) define the methodology for evaluating risk and carrying out the strategy, 2) document necessary costs and resources, 3) explain roles, responsibilities, and coordination of nonfederal stakeholders, and 4) show how the various components relate to national security, homeland security and various other counterterrorism strategies (Elias, 2010, p. 130).

Several books explore specific aviation events and facilities and offer different interpretations of related security strategies. In *The Plane Truth: Airline Crashes, the Media, and Transportation Policy*, Roger Cobb and David Primo explore three accidents: USAir flight 427 (September 1994), ValuJet flight 592 (May 1996), and TWA flight 800 (July 1996) to illustrate how regulatory agencies and Congress reacted to high-profile events with incoherent policy (Cobb & Primo, 2003). Soon after 9/11, Gunnar Kuepper, Chief of Operations for Emergency & Disaster Management Inc., developed a four-part system to assure a proper security strategy, including hazard and threat identification, impact analysis and risk assessment, operational experiences, and cost-benefit studies (Kuepper, 2004).

Some authors explore the value of incorporating security strategy in building architecture. In *Designing Airports for Security: An Analysis of Proposed Changes at LAX*, the Rand Corporation illustrates how airport design as a function of security should consider the effects of attacks before they occur, as in how many casualties an attack would cause, and how an attack would affect operations. By reducing the consequences of a terrorist attack, it is possible to make it less attractive to the potential perpetrators. Small changes in airport procedures or design can have a major effect on the perceived value of an attack to the terrorist. The length of time passengers spend in line is important, because moving people through ticketing, checkpoints, and baggage claim

more rapidly reduces risk (Schell, Chow, & Grammich, 2003). Kennedy International Airport designed the Jet Blue Terminal #5 with security in mind from inception. The security checkpoint is 340 feet wide, which allows passengers to pass through in less than 10 minutes (Dunlap, 2008).

Seeming nonrelated experts argue that relating security to other perspectives can help improve homeland security. In *Beyond Fear*, Bruce Schneier draws an analogy between information technology security and aviation security. His five suggested questions to analyze a security system appear in Table 2 (Schneier, 2003). He also explains how security is both a reality and a feeling that requires different strategies to address each, and that all strategies involve subjective tradeoffs (Schneier, 2003). Roger Grimes in *Computer Security's Dubious Future* points out how complexity inhibits security and makes it easier for an enemy to discover the system's Achilles heel. He quotes Carl von Clausewitz, "As a principle of war, a defender must defend against every possible assault, but an assailant only need exploit a single vulnerability" (Grimes, 2008). These perspectives may be instances of the proverbial "thinking outside the box."

Table 2. How to Analyze a Security System

1.	What assets are you trying to protect?
2.	What are the risks to those assets?
3.	How well does the security solution mitigate those risks?
4.	What other risks does the security solution cause?
5.	What cost and tradeoffs does the security solution impose?

B. GOVERNMENT DIRECTIVES AND POLICY

National and homeland security policy seemed to evolve extremely quickly following 9/11, although not necessarily in a unified manner. Some critics felt more early

stakeholder input would have strengthened policy implementation. Although, time was obviously of the essence, and some proposed components of the *National Aviation Security Strategy* still have not been completed 10 years after 9/11. These documents help understand how the federal government's philosophy evolved aviation security strategy.

In February 2001, George W. Bush began the administration of executive security policy with National Security Presidential Directives, beginning with National Security Presidential Directive 1, *Organization of the National Security Council System*. After 9/11, he used Homeland Security Presidential Directives for homeland security policy. Homeland Security Presidential Directive 1 outlined the operation of the Homeland Security Council. Homeland Security Presidential Directive 9, *Defeating the Terrorist Threat to the United States*, released four days before Homeland Security Presidential Directive 1, basically declared war on the al-Qaeda network.

The federal government seemed to change the size, or at least the organization, of national infrastructure periodically. On December 3, 2003, Homeland Security Presidential Directive 7 superseded Presidential Decision Directive 63, which was issued three years before 9/11. Both defined essential national systems and assets deemed susceptible to terrorist attack and organized the protection of critical infrastructure and key resource. Presidential Decision Directive 63 listed eight critical infrastructure sectors while the *National Strategy for Protection of Critical Infrastructure and Key Assets* lists 11 sectors. The 2007 Homeland Security Presidential Directive 7, *National Infrastructure Protection Plan* outlined 17 sectors.

An updated version of the *National Infrastructure Protection Plan*, released in January 2009, directed each national infrastructure sector to create a working group comprised of members from Government Coordinating Councils and private Sector Coordinating Councils. The working groups were tasks with creating sector specific plans incorporating the eight steps of the System-Based Risk Management process, in the *National Infrastructure Protection Plan* (See Figure 3).

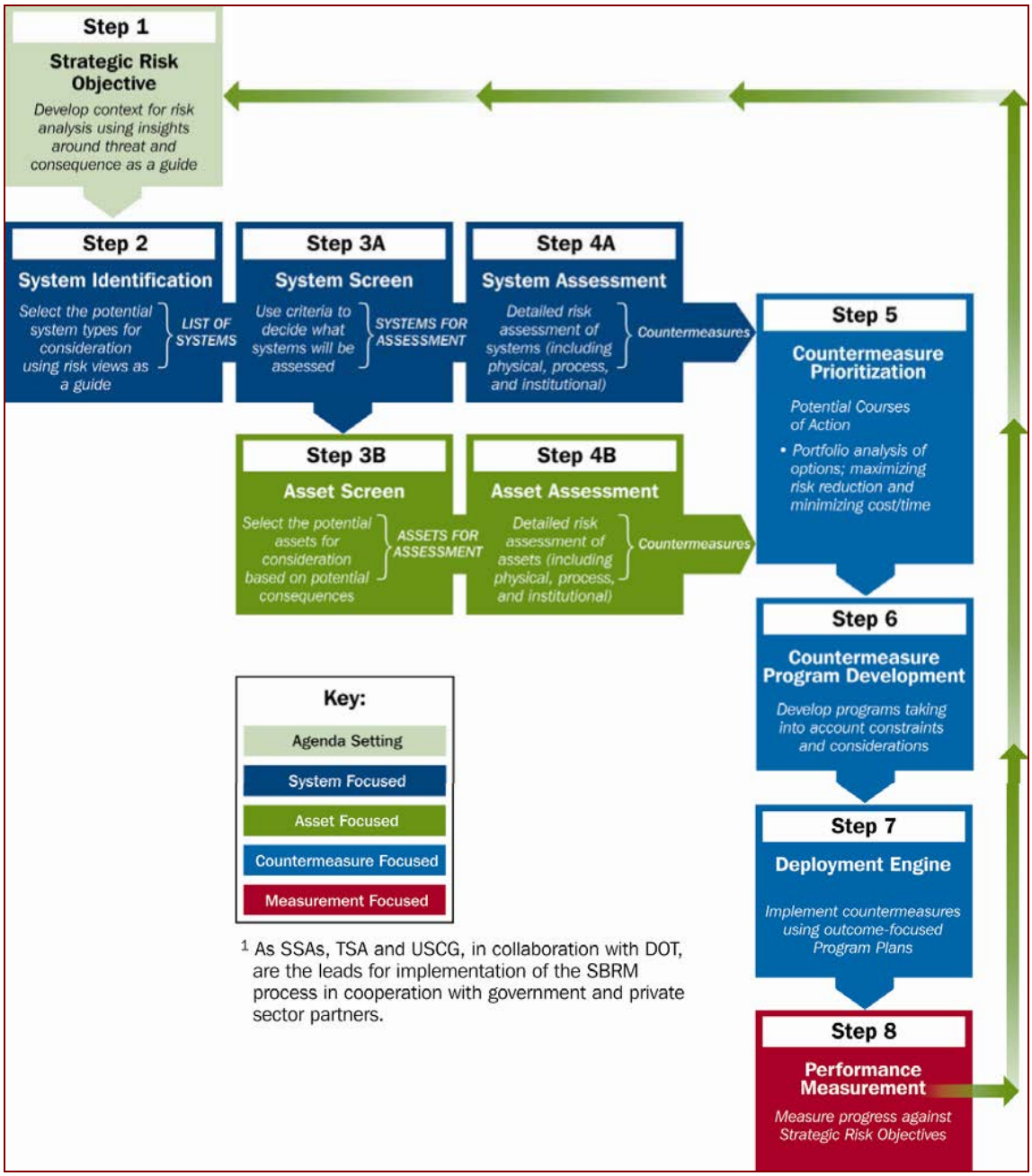
Step 1
Strategic Risk Objective
Develop context for risk analysis using insights around threat and consequence as a guide
Step 2
System Identification
Select the potential system types for consideration using risk views as a guide
LIST OF SYSTEMS
Step 3A
System Screen
Use criteria to decide what systems will be assessed
SYSTEMS FOR ASSESSMENT
Step 4A
System Assessment
Detailed risk assessment of systems (including physical, process, and institutional)
Countermeasures
Step 5
Countermeasure Prioritization
Potential Courses of Action
• Portfolio analysis of options; maximizing risk reduction and minimizing cost/time
Step 3B
Asset Screen
Select the potential assets for consideration based on potential consequences
ASSETS FOR ASSESSMENT
Step 4B
Asset Assessment
Detailed risk assessment of assets (including physical, process, and institutional)
Countermeasures
Step 6
Countermeasure Program Development
Develop programs taking into account constraints and considerations
Step 7
Deployment Engine
Implement countermeasures using outcome-focused Program Plans
Step 8
Performance Measurement
Measure progress against Strategic Risk Objectives
Key:
Agenda Setting
System Focused
Asset Focused
Countermeasure Focused
Measurement Focused
[1] As SSAs, TSA and USCG, in collaboration with DOT, are the leads for implementation of the SBRM process in cooperation with government and private sector partners.

Figure 3. System-Based Risk Management Process (From: Department of Homeland Security 2007)

In June 2006, National Security Presidential Directive 47 and Homeland Security Presidential Directive 16 directed the Secretary of Homeland Security to collaborate with essential agencies and stakeholders to create and implement a *National Strategy for Aviation Security*. Released by the White House in March 2007, this strategy is broadly

based on three objectives: 1) using the full range of assets and capabilities available to prevent the terrorist acts in the air domain, 2) insuring the safe and efficient use of the air domain, and 3) facilitating travel and commerce (National Strategy for Aviation Security, 2007).

Later that year, the Department of Homeland Security began creating a set of supporting plans to the *National Strategy for Aviation Security* that provide a situational framework for implementing the core strategy before, during, and after possible terrorist events (Figure 4). The first three plans address day-to-day security measures and programs to reduce aviation sector vulnerability to terrorist or criminal acts. The *Aviation Transportation System Security Plan* is focused on identifying and vetting customers, contractors, and employees of the aviation transportation system. It also addresses preventing use of the system as a weapon, and hardening critical elements of the system against other forms of attack. The *Air Domain Surveillance and Intelligence Integration Plan* coordinates the gathering, analysis, and dissemination of intelligence to appropriate stakeholders, which thereby enhances the system security plan. Worldwide, the *International Aviation Threat Reduction Plan* and the *International Outreach Plan* guide cooperative efforts with other nations to improve global aviation security.

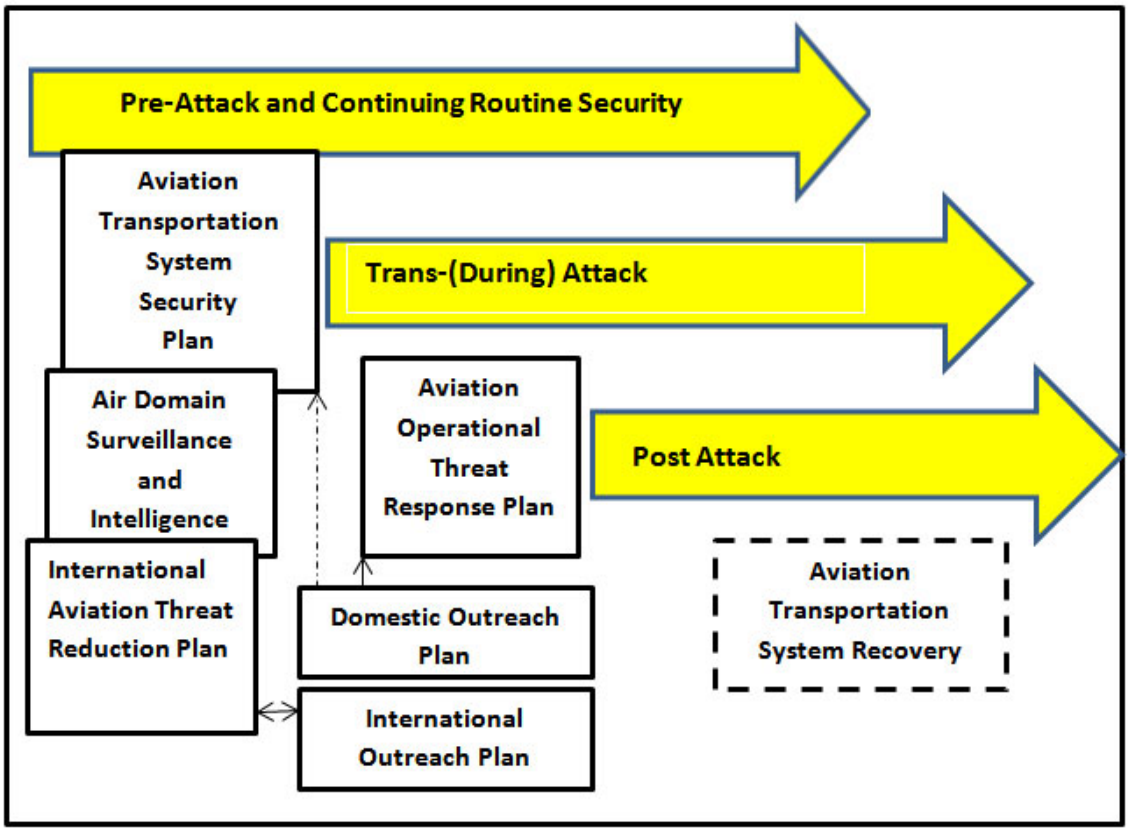

Figure 4. Supporting Plans to the National Strategy for Aviation Security

The *Aviation Operational Threat Response Plan* is activated once a terrorist or criminal attack occurs, which facilitates immediate actions to mitigate a wide range of possible security threats. This plan is augmented by the *Domestic Outreach Plan*, which outlines communication with state, local, and tribal government, as well as the private sector, to bring their resources into play. Finally, the *Aviation Transportation System Recovery Plan* is being developed to facilitate the aviation sector's continuity of operations and minimize economic impact after a terrorist event (Elias, 2010).

C. CONGRESSIONAL REPORTS

This thesis references numerous U.S. Government Accountably Office Reports, Congressional Research Service Reports, and Congressional Staff Reports. The Government Accountably Office supplies Congress with independent analysis of government programs and activities according to the Budget and Accounting Act of

1921. These reports include generic recommendations and options and follow up analysis on the extent and results of proposals being implemented. The Congressional Research Service is a branch of the Library of Congress that does policy research for members of Congress, congressional committees, and staff. Finally, legislative staffers conduct research and analysis on policy issues and assist in designing and implementing strategies to accomplish the legislative goals of their members of Congress. It needs to be noted that all these reports are subject to political influence and should be interpreted accordingly.

Fifteen Government Accountably Office reports were reviewed for this thesis, beginning with the *Aviation Safety and Security—Challenges to Implementing the Recommendations of the White House Commission on Aviation Safety and Security*, released March 5, 1997. Nearly every report recommended a "comprehensive strategy" with "clear goals and objectives, measureable performance criteria…, (and) a monitoring, evaluation, and reporting system…" (Dillingham, 1997).

From 2007 to 2009, the Government Accountably Office evaluated how well the Transportation Security Administration (TSA) complied with the *National Infrastructure Protection Plan* directive to access risk and improve airport perimeter security. Its conclusion found the administration's effort to measure security according to cost, benefit, and impact was imprecise and disorganized. TSA contended it would address this process with a systems-based approach in the near future. Furthermore, the Government Accountably Office noted "limited usefulness" of TSA's past efforts due to the lack of adequate goals or objectives, milestones, and documentation and recommended designing and implementing an analysis process based on accepted risk management and public administration principles. It also indicated the need for a national strategy specifically focused on making airport security decisions (GAO, 2009).

The latest Government Accountably Office report referenced was an audit of the first Quadrennial Homeland Security Review, released in September of 2011. It noted the Department of Homeland Security had not yet conducted a National Risk Assessment and that many stakeholder participants felt the process had been rushed, which limited their input (GAO Highlights, 2011).

Five Congressional Research Service reports were included in this literature reviewed. The *Homeland Security Act of 2002: Legislative History and Pagination Key* included a brief history of the incidents and processes preceding the passage of the act. The *National Aviation Security Policy, Strategy, and Mode-Specific Plans: Background and considerations for Congress*, released in 2009, summarized the *National Strategy for Aviation Security* for members of Congress, which suggested five areas for further congressional investigation (Table 3) (Elias, 2008).

Table 3. Suggested Congressional Investigations

1)	Underlying Risk Assumptions
2)	Security System Sustainability
3)	Reactive Planning
4)	Comprehensive Security Framework
5)	Budgetary Alignment

D. PUBLIC ADMINISTRATION AND PERFORMANCE MEASUREMENT

According to management authority, Peter Drucker, whether an organization is a private for-profit business, a non-profit charity, or a government institution, it must employee specific management principles to be effective. Examining these principles should help determine the strengths, weaknesses, and opportunities of current aviation security. To quote Drucker, "Management is the specific and distinguishing organ of any and all organizations." He also notes the most important management responsibility is to create "targets and yardsticks," enabling employees to know how well they have achieved organizational objectives (Peter F. Drucker Literary Trust, 2008). In *Reinventing Government*, David Osborne and Ted Gaebler wrote, "If you don't measure results, you can't determine success from failure" (Gaelber & Osborne, 1992, p. 142).

Most of the books and articles concerning metrics of public and government organizations were written after World War II. Nevertheless, early analyses of industrial productivity began with Frederick Taylor's reports of time-and-motion studies done in 1881. Taylor referred to his theories as "Scientific Management," which was designed to reduce work and eliminate waste (Peter F. Drucker Literary Trust, 2008).

In *Airport Security, High Reliability and the Problem of Rationality*, George Frederickson and Todd LaPorte relate how the principles of high–reliability organizations could apply to airport security operations. Contemporary decision theory, based on the study of error-tolerant organizations and nearly error-free operations could, in theory, improve air travel security. They examine numerous innovative management concepts including the value of high technical competence, sustained performance, decentralized authority, and rewarding employees that discover and correct errors (LaPorte & Frederickson, 2002).

The International City/County Management Association has been actively involved in measuring performance for since the late 1980s (Hatry et al., 1992). They recommend measuring fire department effectiveness by collecting and comparing loss data over time and across similar communities, then correcting for external variables, such as socio-economic circumstances. Similar adjustments may be prudent when applying aviation security metrics. One Government Accountability Office report noted an issue with TSA not accounting for different categories of airports or employee numbers in the design criteria of employee security pilot programs (GAO, 2009).

E. ACADEMIC RESEARCH

Some academics maintain, "If you can't measure it, it does not exist" (Brown 2010). Scientific methodology can obviously play a large part in comparing and contrasting specific aspects of security strategy and implementation. Once again, however, politics may have some influence and should be considered when interpreting academic research concerning strategy.

Norman Schneidewind applied statistical risk analysis to airport security by using randomized hypothetical and factual data, and compensated with sensitivity analysis to understand airport security better. He attempted to identify weak points, such as the "passenger flow through the ticket counter, security station, and gate," and quantify the probability of detecting terrorists at each location. The model could possibly help evaluate systemic changes in security policy (Schneidewind, 2006).

Economists Geoffrey Heal and Howard Kunreuther used an analogy of airport security to address risk analysis with the Nash equilibrium gaming model. They demonstrated how action taken by any participant affects risk to all participants. This research may have application in the international outreach element of the Aviation Security Plan (Kunreuthe & Heal, 2007).

Another article in the same journal evaluated the cost effectiveness of using one versus two baggage-screening devices. Dr. Qianmei Feng, a fellow with the University of Houston, used probability theory and statistical optimization to conclude, "A two-device baggage-screening system should be deployed rather than a single-device system, as a properly arranged two-device system outperforms a single-device system in terms of the level of security and cost effectiveness" (Feng 2007). This research indicated the increased reliability justifies the investment in multiple systems. It may be possible to extrapolate this conclusion into other security components.

In their article, "Is this Paper Dangerous? Balancing Secrecy and Openness in Counterterrorism," Jacob N. Shapiro and David A. Siegel ask, "How open should government be when aggressive non-state actors seek to take advantage of information shared in the name of good governance or the public's right to know?" To answer this, they surveyed 186 U.S. federal, state, local, and industry homeland security officials. The survey included a simple open-ended question: "How do you think about the tradeoff between secrecy and openness in Homeland Security?" and several questions to measure how respondents perceived specific variables related to "Strategic Information Release." Shapiro and Siegel determined, "information sharing can improve the efficiency of protective spending" and "much more attention should be paid to how openness can help government identify vulnerabilities" (Shapiro & Siegel, 2010).

U-map, an area of academic research focused on transparency, has potential use in data analysis of security. It is an ongoing project in Europe used to classify and compare higher education institutions. U-Map employs sunburst charts to compare information about universities, which makes it easy to understand and compare institutions. The charts present statistics in six major categories: teaching and learning, student profiles, knowledge exchange, international orientation, research involvement, and regional engagement. The chart further subdivides each category, which are measured in broad general ranges (See Figure 5). For instance, teaching and learning includes subject areas covered (measured as comprehensive, broad, specialized, and none), degrees level focus, orientation of degree, and expenditures on teaching. The interactive website allows researchers to drill down easily, which facilitates decision making (Center for Higher Education Policy Studies, 2008).

University "A" University "B"

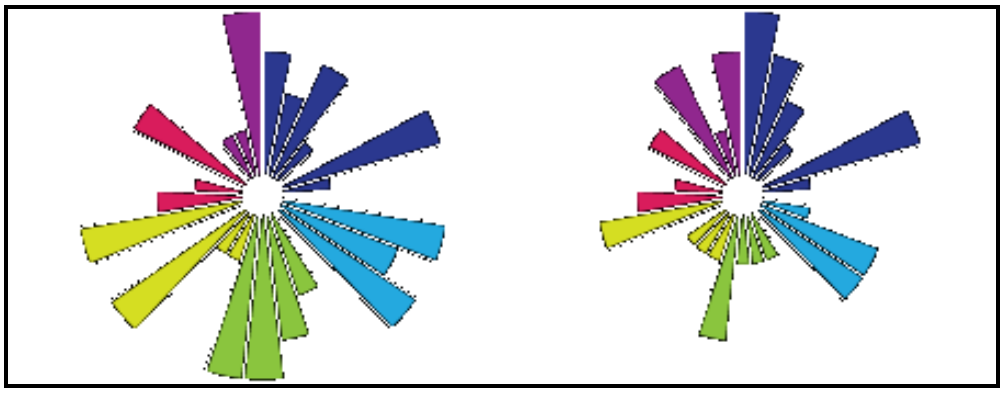

Figure 5. U-Map Sunburst Charts

F. FIRE PREVENTION LITERATURE

David Rasbash looked at fire safety from an engineering perspective in *Evaluation of Fire Safety*. He attempted to quantify risk, or evaluate the potential of a hazard by distinguishing the expected frequency of an event and the severity of the associated consequences to compare the costs of fire with other hazards, the expense of mitigation and control, as well as the value and tradeoffs of designed

safety. To illustrate how fire safety interacts with other hazards, the theoretical maximum fire safety benefit "A" considering other hazards, is calculated with the following equation: A=(fd +fc)-(hd + hc), with "fd" being the detriment (direct and indirect costs) caused by a fire, "fc" the cost (dollars, time, and inconvenience) of fire safety, "hd" the detriment of other hazards, and "hc" being the cost of other hazard prevention. Obviously, many of these values are not easily quantified. Rasbash believes fire is the "most complex phenomenon occurring in nature" and suggests a 20-step process to design a fire safety program (Table 4). He also outlines two quantitative approaches to evaluating fire safety, point schemes, referred to as rating schemes, and mathematical modeling (Rasbash, Ramachandran, Kandola, Watts, & Law, 2004).

Table 4. Steps to Design a Fire Safety Program (From: Rasbash et al., 2004)

1. Define the fire hazard area.
1a. Identify people, property, and processes at risk from fire and explosion incidents within the fire hazard area.
2. Define the fire safety objectives.
3. Assess materials that can burn.
4. Assess sources of ignition.
5. Assess the conditions of fire spread that would lead to an established fire.
6. Assess agents that cause fire (i.e., that bring 3, 4, 5 together).
7. Estimate the probability of fires being caused.
8. Assess the means available of limiting fire, (1) active means (2) passive means.
9. Estimate the courses of fire behavior.
10. Assess the harmful agents produced by fires and their capacity to harm people and property
11. Estimate the production and range of action of harmful agents produced by fires.
12. Assess methods of protection against the harmful agents.
13. Estimate the direct detriment to people and property that may be caused by fires.
14. Assess available methods of protecting people and processes from the indirect effects caused by direct detriment.
15. Estimate indirect detriment.
16. Judge whether estimated direct and indirect detriment comply with fire safety objectives. If Step 16 shows that the objectives of fire safety are not met, then carry out the following steps.
17. Postulate changes in the fire safety situation, for example in the precautions taken.
18. Estimate the effect of changes on achievement of fire safety objectives.
19. Define an acceptable method of achieving objectives, taking into account cost and convenience.
20. Formulate and express fire safety requirements.

In *Fire Protection Engineering* magazine, Arthur E. Cote explained how after a particularly notorious high-rise fire in New York City, the General Services Administration convened an international conference in 1971 to consider standards for high-rise building fire protection systems. The conference also articulated the need for a "total systems concepts approach" to fire safety that resulted in the National Fire Protection Association creating the 550 standard and the Fire Safety Concepts Tree (Figure 6). The tree outlines two methods to achieve fire safety objectives by first preventing fire, and second, managing the fire impact by mitigating the fire and/or securing the exposed people and property (Cote, 2008).

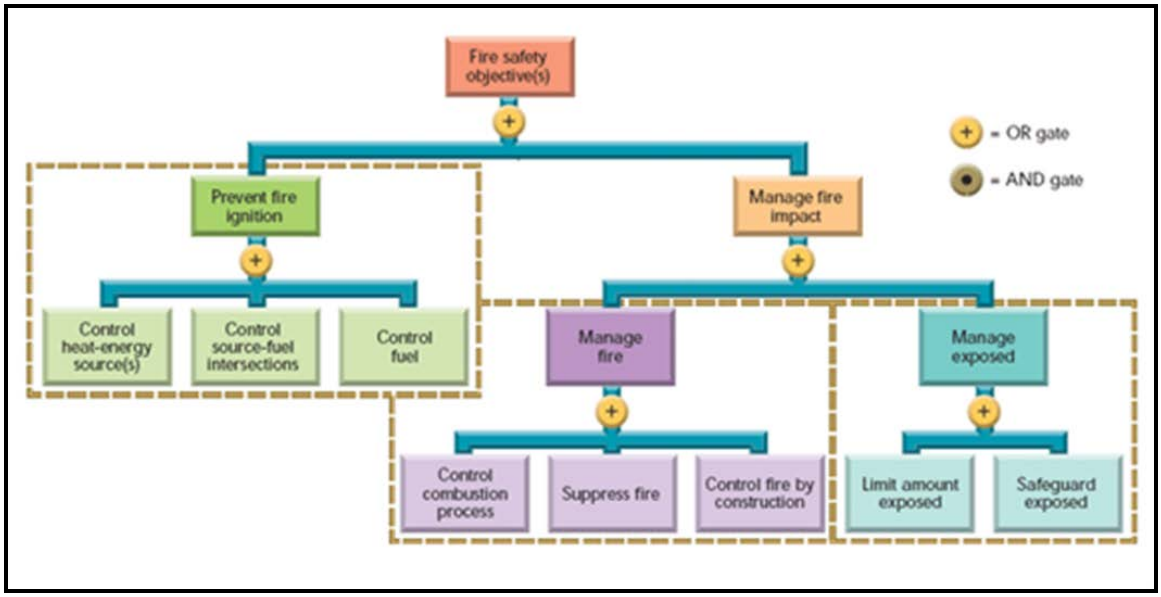

Figure 6. Fire Safety Concepts Tree

G. CONCLUSION

While an abundance of literature is relevant to airport security, and much of it calls for measuring outcomes, the actual structure and application of assessing the relative effectiveness of security still seems less than robust. The goal of this thesis is to investigate incorporating public administration policy-analysis tools and the fire safety

consensus standard model to guide aviation security. The literature suggests these systems may be compatible with the System Based Risk Management framework and the flexibility and randomness strategy to reduce potential terrorist exploitation.

III. METHODOLOGY

A. OVERVIEW

The methodology employed in this thesis borrows from policy analysis and formative program evaluation. The purpose is to investigate how airport security programs and policies are being evaluated and how those evaluation processes could be improved. The extensive literature review provided a sense of the current status of scholarship in this area, as well an opportunity to identify smart practices used in fire safety. The research component of this thesis is qualitative and employs a two round Delphi survey of 10 members of the Transportation Security Services Committee of the American Association of Airport Executives. This methodology is suitable to answer the research questions, as members of this committee are recognized subject matter experts in the field of airport security, and as a body, help develop policy recommendations for TSA.

Sixty-seven members of the committee were contacted by phone and asked to participate in the survey. Thirty-eight agreed to read the first round and the three questions along with informed consent forms were emailed to them. Ten members responded to the first round of the survey. After summarizing and analyzing the answers, the questions for the second round were formulated. The summaries and unidentified individual responses were emailed back to the respondents along with the three questions of the second round, to which seven members responded. The anonymous responses of both rounds are included in the appendix. The summaries are included in the Analysis and Findings chapter.

B. SURVEY

1. Round One Survey Questions

1. What criteria do you currently use to judge the efficiency and effectiveness of your security policy and procedures?
2. Which criteria do you consider most useful and why?

3. What metrics pertaining to security policy or procedures would you like to see employed?

2. Round Two Survey Questions

1. According to the first round, there is an apparent desire and willingness to share security performance data. Do you believe a secure web based, professional network, dedicated to airport security information sharing, would be feasible and worth the effort? Why?
2. Is the International Civil Aviation Organization Security Audit Program a valuable tool? Why?
3. Considering the concerns and ideas expressed in the survey's first round, what methods would best help determine how to allocate security resources? Why?

C. LIMITS OF THE EMPLOYED METHODOLOGY

The results of these surveys should be compared and interpreted with some slight to moderate uncertainty. Not all the responses were entirely candid, as demonstrated by some of the qualified answers. In addition, the survey population was fairly limited, possibly due to security concerns of the potential participants, and finally, no adjustment was made for the contributing airport's operational differences.

The original methodology chosen was interviewing the Security Managers at airports selected according to similar demographics. However, it became apparent very early that the lack of cooperation would mandate a different process. The Delphi survey was substituted. However, the survey presented a comparable challenge. Shortly after sending out the surveys, the TSA called and inquired about who had been contacted, the purpose of the survey, and the nature of the research credentials. TSA directed to stop further surveys, until they verified the validity of the research. One week later, authorization to continue was granted, with the caveat that all participants had been advised to seek TSA clarification before divulging any potentially sensitive security information. The implication for this and future research is that less than full transparency or complete data makes it difficult to improve public safety policy.

D. PROPOSED RECOMMENDATION

The results of the literature review and surveys will be combined to design a recommended performance measurement system for one aspect of airport security. It will be aligned with the National Infrastructure Protection Plan and System Based Risk Management and will consider relevant national standards, local factors and criteria, and established public safety measurement concepts that can be adapted. The process will involve defining, evaluating and selecting the proper performance indicators and methodology, with a focus on creative thinking, seeking new knowledge, avoiding metricizing, and maximizing utility, while addressing skepticism.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS/FINDINGS

A. ANALYSIS INTRODUCTION

In this chapter, the results of the survey are analyzed by categorizing, comparing, and graphing the responses to help illustrate key findings. Specific comments and phrases from the participants are included in quotes when relevant. The complete survey results are presented in the appendix. When relevant, the analysis is compared with appropriate fire safety evaluation concepts and contemporary performance measurement theory gathered from the literature review.

Only 10 of the 68 members of the American Association of Airport Executives Transportation Security Services Committee responded to the first round of the survey and seven responded to the second round. The limitations of the survey are noted in the methodology chapter.

1. First Round Survey

- Question #1. What criteria do you currently use to judge the efficiency and effectiveness of Airport security policies and programs?

Participants listed a moderate range of measures, including calculating average times passengers wait in lines, assessing financial expenditure per passenger for security programs, and operational losses due to security events. This question yielded 34 data segments, which were classified into six basic categories. Four segments fit in multiple categories (Figure 7).

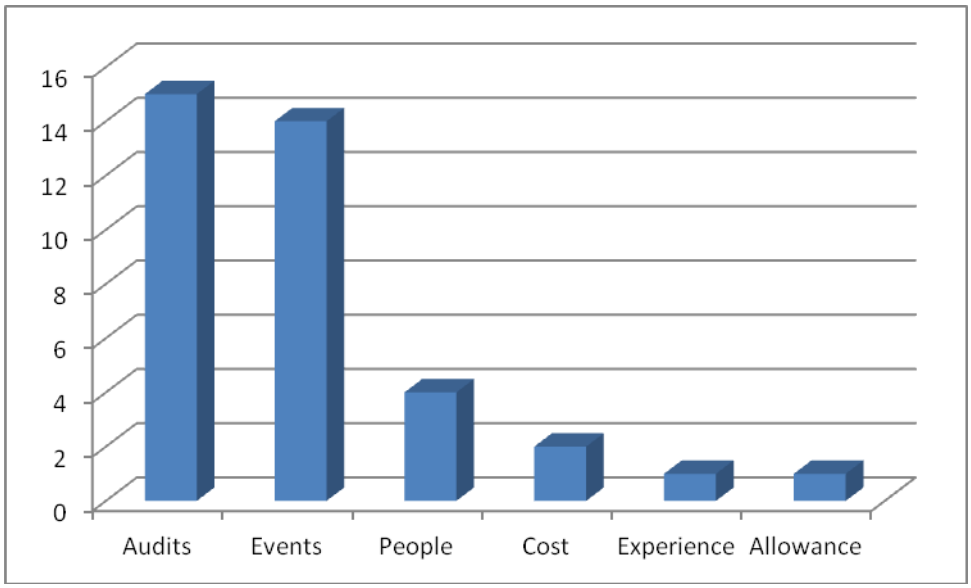

Figure 7. What Criteria Do You Currently Use to Judge the Efficiency and Effectiveness of Airport Security Policies and Programs?

The 15 (39%) segments in the primary category, "Audits," referred to any activity related to a formal examination or systematic checks, including checklist, quantified tests, or exercise results. It may be noteworthy that only one respondent mentioned the International Civil Aviation Organization Security Audit Program.

The second most common category, "Events" included all activities related to security violations or breaches, which occurred 14 times (36%). This category could be subdivided into number of events or items confiscated and times required to respond to and assess security incidents.

Human factors, "People" were included as the chosen metric four times (10.53%), either as the number of employees or passengers screened, employees issued badges, the time required to do so, or the cost per passenger. Cost per passenger also fit in the category of "Cost," which included money spent or resources expended, and was mentioned twice (5.26%).

The last two categories, "Experience" and "Allowance" occurred only once

(2.63%) each and incorporated expert experience and allowed for differences in the type of airport. While not specific metric activities, because they were significant filters, both were included in the analysis.

Comparing apples to oranges will not provide useful metrics. The differences in physical layout of airport access and critical resources, or the number of passengers and employees can dramatically affect the value of particular mitigation strategies. Several respondents raised this issue in answering question #3. Furthermore, the nuances of these variances will often only be obvious to individuals with direct practical experience in aviation operations and security.

- Question #2. Which of these do you consider most useful and why?

This question attempted to determine how certain metrics are considered more productive. The participants indicated 12 "most useful" security criteria that were condensed into four subject categories using the same definitions as question one. Again, some answers fit into multiple categories. The 13 associated justification categories were abridged into five groups. (One category was nil or no justification)

The chart in Figure 8 indicates the relative weight of each criterion by the size of the text box, and the related reasons via connecting arrows. The criteria categories appear in the left column and the associated reasons in the right. The category "Cost" referred to a measurement criterion and a reason to gauge security, and therefore, occurred in both columns. Participant "F" justified analyzing "regulatory compliance" as a way to "reduce financial risk." While, "I" specified computing "cost per boarded passenger and operational costs to tenants…is a basic measure of efficiency." (Note: this participant also noted three other methods as "Most Useful")

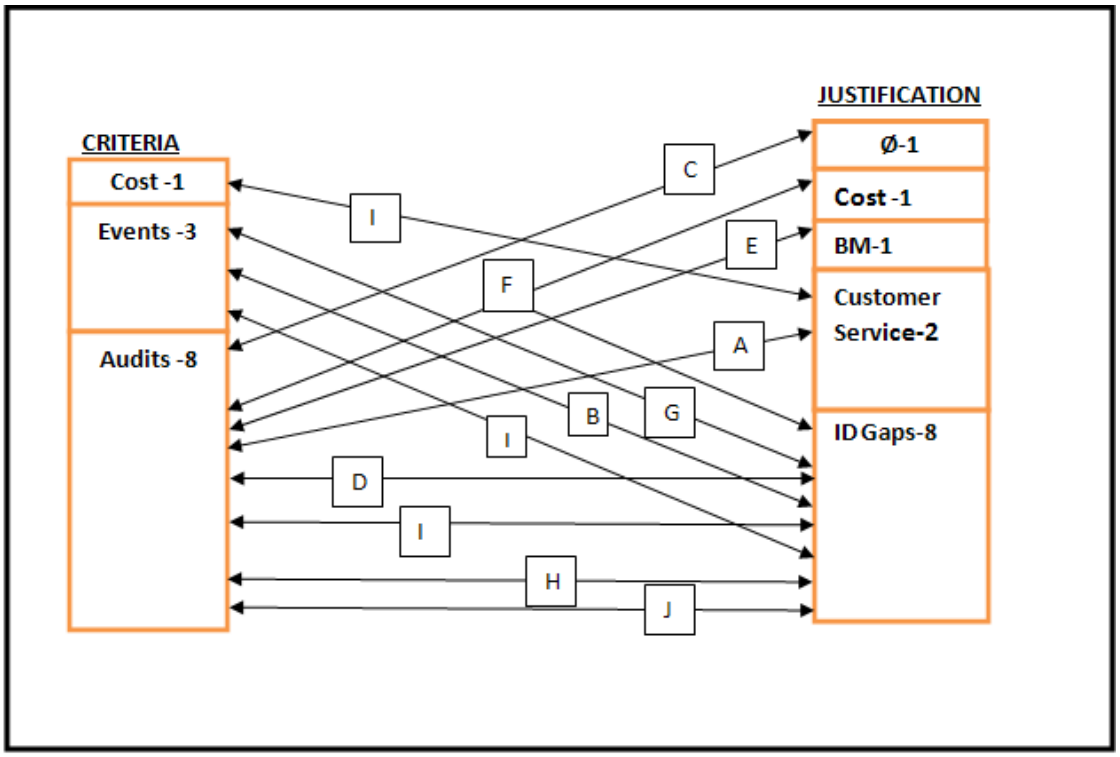

Figure 8. Which of These Do You Consider Most Useful and Why?

"Audit" was by far the most popular criterion, (8), although the International Civil Aviation Organization Security Audit Program only came up once and did not relate to any justifications. The participant possibly felt it was self-explanatory. Half of the "Audit" responses (4) related to "Identifying Gaps." This justification elicited the most responses (8). The other 50% was equally distributed, one each to the remaining four justification categories, customer service, establishing benchmarks, cost, and nil. Respondent "I" split the justification between "cost" and "Identifying Gaps."

Monitoring security "Events" was the second most prevalent category. It included three responses that were all related to "Identifying Gaps." Customer Service was the second most prevailing justification with two responses, one related to "Audit" and the other to "Cost."

The overwhelming majority of survey participants felt some type audit procedure should be used to identify gaps in the security system. In addition, the "Audit" criterion was related to every justification category. Furthermore, every criterion with the exception cost was validated as most useful because they could identify gaps in security.

- Question # 3 What metrics pertaining to security policy or procedures would you like to see employed? Why?

The third question was designed to direct participants beyond current applications and encourages original thought. One responder actually alluded to innovation as "operators taking initiative"… (If not) "Penalized by TSA." A word cloud, shown in Figure 9, was employed to analyze the six most frequent terms in the responses.

area (4) awareness (3) categories (5) efforts (3) employees (4) enforcement (3) environment (3) improve (3) incident (3) law (3) location (3) maintaining (3) measure (3) operators (3) performance (3) personnel (4) procedures (3) program (9) public (7) reporting (4) required (3) risk (3) safety (3) score (3) systems (11) test (3) training (7) tsa (7)

Figure 9. What Metrics … Would You Like to See Employed?

The most common significant word, "System" was used 11 times. A review of the ideas associated with this term indicated the respondents thought overall security included many components working together in a "system. Furthermore, those components could be measured in some meaningful way. Although two of the respondents were not convinced that the quality of security could be quantified effectively, they still felt the "system" should be analyzed whenever possible. The

resistance to metrics was based on the possibility expert analysis would be more apt to discover gaps in the system and changing situations could negate investment in specific programs.

The term “Program” referred to individual components within the security “system” and was the second most used significant word, and occurred nine times. (Including the plural form) For example, “Public and employee security awareness programs.” The primary knowledge gained from examining the use of this term was each component should be evaluated separately as it is likely competing with other “programs” for limited resources.

The fifth rank was a three-way tie with “Public,” “Training,” and “TSA,” each garnering seven uses. A single respondent used the term “Public” seven times. The first three referred to “public safety personnel,” and the latter four to the value of developing and monitoring “public awareness” programs. In addition, only one respondent mentioned “training” but he used it seven times. He not only felt it was important to document and evaluate security related training, but suggested the use of technology could vastly improve training.

Three respondents recommended “TSA” record, catalog, and share data about security events with individual airports to improve local security analysis. One reply suggested, “TSA” … “employ threat assessment and risk analysis,” but adjust the analysis for each different category of airports.

“Categories” of airports was ranked sixth, and was mentioned five times (including the singular). Three respondents referred to comparing metrics according to the “category” of airports. Two indicated a need for standards or benchmarks because, “programs… (vary) greatly by airport even within a category and thus comparisons are difficult.”

Although “audit” or “testing” did not appear in the word cloud, two participants mentioned them. Other suggestions included comparing the quantity and use of security personnel, systems, training, and equipment.

2. Second Round Survey

- Question # 4 According to the first round, there is an apparent desire and willingness to share security performance data. Do you believe a secure web based, professional network, dedicated to airport security information sharing, would be feasible and worth the effort? Why?

The participants were affirmative and unanimous that sharing data was feasible and valuable. Nevertheless, when responding to the "why" sharing data was desirable, the participants raised four types of concerns: utility, responsibility, credibility, and security. Utility encompassed analysis or "connecting the dots," benchmarking, and working in "real time. Responsibility referred to who would "host the website." Credibility denoted a potential lack of trust, which referred to data from stakeholders. Security was also related to trust. However, rather than questioning the data, it referred to the ability of stakeholders to maintain the secrecy of analysis products. Although the survey results indicated solidarity to the concept of sharing, the ideas about application were extremely lopsided.

Utility was raised nine times when the three components were summed, which may be an indication that the respondents believed it was important to incorporate analysis of the data by as many participants as possible, compare the findings, and use the best to set standards. Furthermore, as terrorists are always looking to take advantage of gaps in security, noting "patterns" possibly connected to "events" or "significant dates" could be extremely "time relevant." The graph (Figure 10) indicates responses by the individual components, "benchmarking" (4), "analysis" (3), and "real-time" (2).

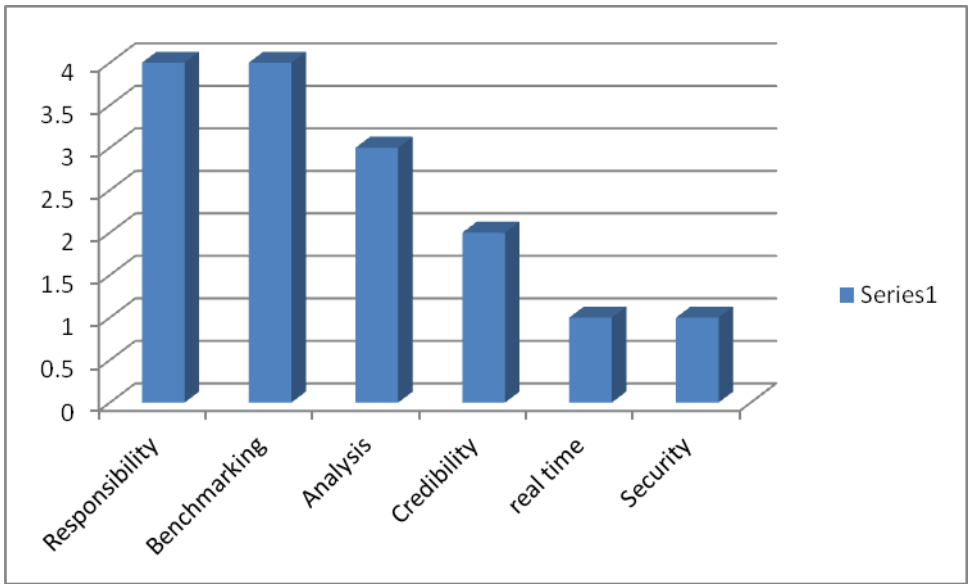

Figure 10. Why a Secure Web-Based, Professional Network, Dedicated to Airport Security Information Sharing, Would Be Feasible and Worth the Effort?

Those concerned about "responsibility" seemed to indicate stakeholders needed to participate. One participant suggested an airport operators association, for instance, the American Association of Airport Executives should be involved in sharing data. Two recommended that TSA should "publish metrics…in conjunction with stakeholders." One reported TSA already has a "SSI" protected website. "Responsibility" was the second highest response with a total of four.

"Credibility" placed third with three respondents expressing doubt about data obtained voluntary. The National Fire Protection Association has a similar problem, as discretionary reporting participation is less than half the fire departments in the country, which yields conclusions based on estimated numbers. Although in general, the fire service believes national fire reporting data accurately indicates trends, this survey seems to show respondents think aviation security should be held to a higher standard.

Only two respondents mentioned "Security." One survey participant believed possible distrust by federal authorities would minimize any value, as stakeholders would be denied access to sensitive security information. Another participant recommended requiring security clearance before allowing access to the shared platform.

This question overwhelmingly received optimistic answers. Everyone thought information sharing would be beneficial. Three separate benefits were mentioned. Although two separate problems were raised, both were related to trust and the proposed solutions seemed relatively simple and logical.

- Question # 5 Is the International Civil Aviation Organization Security Audit Program a valuable tool?

Only two participants expressed personal knowledge and understanding of the program, but they disagreed as to the value of the program. One stated it was "too broad" for local airport operators security programs, while the other called it "the baseline of security elements." This second respondent also suggested that it had significant "Gaps." A third participant believed that the International Civil Aviation Organization security audit was a good fit for U.S. airports, but his nonspecific reasoning indicated a lack of direct experience with it. The other four respondents indicated they were "unfamiliar with it" or had "not worked" with it. Although, one had looked it up on line before responding and thought it would be a "good starting point." Finally, one had used another audit "that was developed locally." See Figure 11.

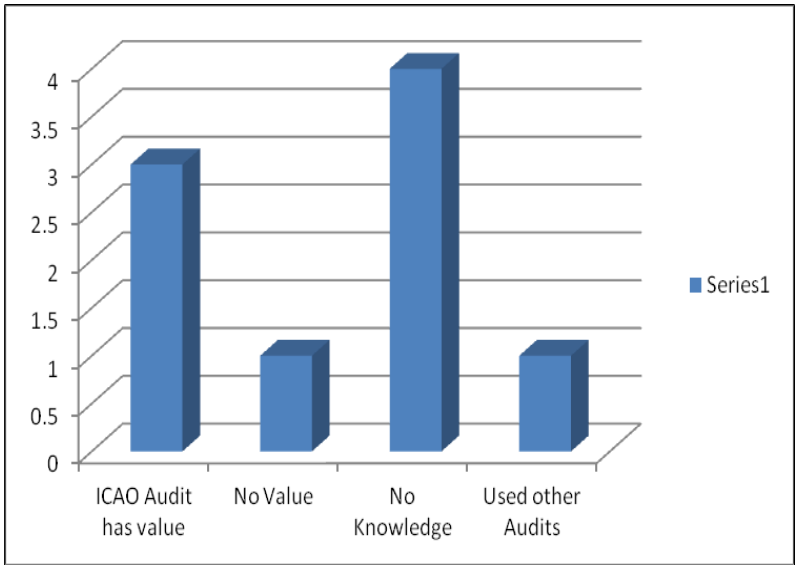

Figure 11. Is the International Civil Aviation Organization Security Audit Program a Valuable Tool?

- Question # 6 Considering the concerns and ideas expressed in the survey's first round, what methods would best help determine how to allocate security resources?

"Assessment" was by far the most popular method chosen. Four participants referred to risk analysis or vulnerability assessment, which likely meant the comprehensive TSA risk assessment for airport security was based on the risk management framework in the National Infrastructure Protection Plan. However, two of the four participants in this category qualified their answers by suggesting using national and local components of risk assessment to allocate resources. One other participant referred to differences based on "areas of the country." In this question, this type response was listed as "Adjust."

Systematic examination of other kinds of data, such as "analysis of operational losses" or "covert testing," is included in the "Audit" category. Only one participant stated that "Audit" methods were best. This person also had the only response related to cost-benefit analysis, and also included "employee security awareness programs" as a good way to determine resource allocation. This response may indicate, however, that the question was misunderstood and meant it would be good to allocate resources to this program. One participant indicated an "intelligence network" that included more than aviation events would be a good way to regulate resource allocation, which is categorized as "Network." Figure 12 illustrates the answers.

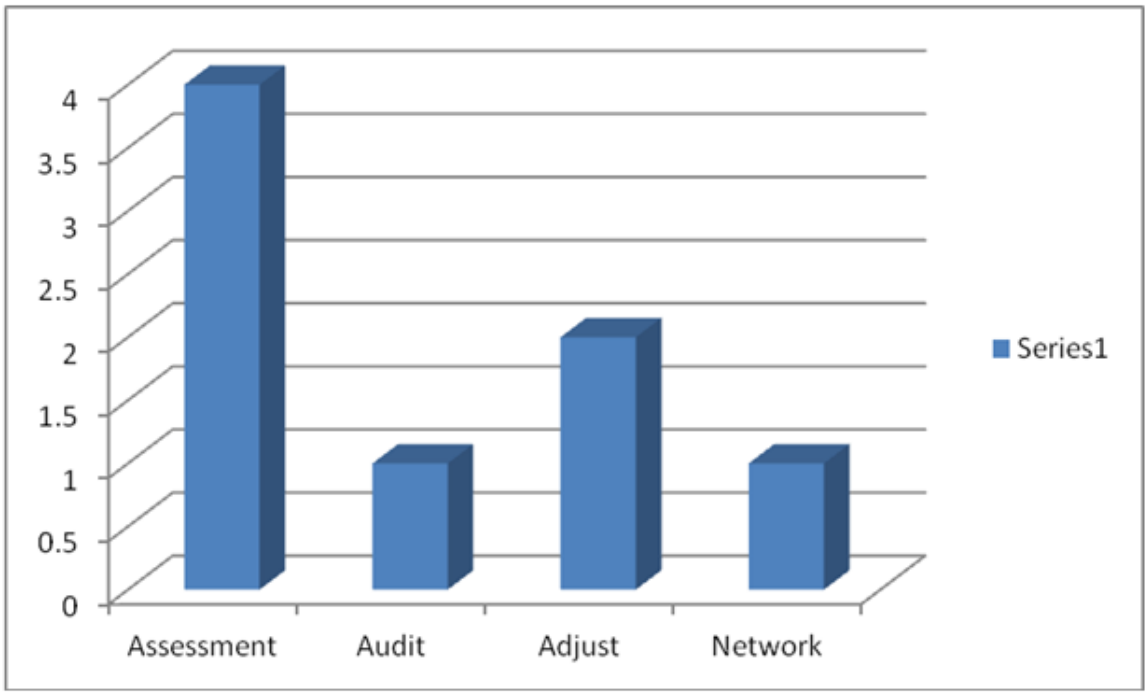

Figure 12. What Methods Would Best Help Determine How to Allocate Security Resources?

B. FINDINGS

To what extent is commercial airport security currently measured and how should it be measured? While low hanging data is significant, what is missing can often provide just as much or more important insight. This survey indicated the primary concerns of security practitioners are currently audits, breeches, regulatory compliance, and information sharing. However, the data did not reflect considerations that management theory would seem to indicate belong in a discussion of security metrics. Technology (or dependence on), objectives (mission), and management are important issues in the execution of security strategies. When compared to contemporary management and performance measurement theory, what do these patterns and anomalies suggest?

Based on the survey results, it can be assumed that today most, if not all commercial airports, primarily use audits that should include assessment of statutory and code compliance, and security breech statistical reporting, to gauge the effectiveness of security. While the survey did not address specific mechanics of audit and breech reports,

it is likely these measures consider output and outcome components, and are therefore, necessary and important tools to indicate how well some parts of the multilayered strategy work. Hopefully, these measures are customized to each facility and process to some extent that would increase reliability and utility. Future research should facilitate adaption and improvement of these types of measures.

Many numerous explanations may exist as to why a number of significant factors were not mentioned in the survey. Although the study did not directly address comparing security technology, objectives, or management, these topics may be measured in most audit processes. Nevertheless, it seems odd that none of the respondents believed these issues important enough to mention specifically. The respondents may have assumed a consensus exists as to what "successful" security should look like, and linking measurements to mission or management was redundant. However, the literature review indicates a significant divergence of what may be considered good security. At the same time, the literature illustrates that a clear understanding of mission is critical to developing and using appropriate measurements. "Identify organizational mandates" and "Clarify organizational mission and values" are steps two and three in John Bryson's "Ten Step Strategic Planning Process" (Bryson, 2004, p. 32). In *Measuring Performance in Public and Nonprofit Organizations*, Theodore Poister considers mission, goals, and objectives, the basis of meaningful measures (Poister 2003, p. 58).

While the starting point for an effective strategy is the organizational mission, and desired outcomes are the destination, planning and implementation is the journey and perhaps offers the greatest prospect for improvement. The general concern with desired outputs and outcomes may have caused management to be overlooked as a measurement consideration in this survey. However, no one would argue management is a major influence on the effectiveness of any program and should be examined beyond a summative assessment. John Bryson recommends achieving success by monitoring "instrumental subordinate outcomes" along the way to the desired end of "achievement of organizational goals and heightened stakeholder satisfaction" (Bryson, 2004, p. 239). It may be extremely important to measure how management applies accepted and innovative leadership principles.

This survey confirms numerous opportunities exist to improve aviation security and suggests beginning in four areas. Systematic audits, including training security practitioners in the theory behind different types of assessments, should continue to be used, increased, and improved. Breech reporting statistics should include comparative performance data in addition to accounts of activities. Electronic information sharing should be expanded to facilitate benchmarking technology and individual roles, innovation, and linking measurements to goals and objectives. Management should be evaluated at all levels, including factoring in individual experience and employee development programs. As criminals and terrorists constantly modify their strategy and tactics, aviation security must continuously measure performance at all levels to keep at least one step ahead.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

Peter Drucker once said, “no institution can possibly survive if it needs geniuses or supermen to manage it. It must be organized in such a way as to be able to get along under a leadership composed of average human beings” (Smith, 2004). This thesis concludes that an opportunity does exist to improve commercial airport security by testing innovative management and measuring the results. As the responsible regulatory agency, TSA should guide and oversee an industry-wide effort to advance this change, which means developing standards for adequate management performance, communicating those measures effectively, allowing innovation, monitoring results, and adjusting security standards as needed.

This thesis identifies public administration and performance measurement principles with the potential to increase effectiveness and efficiency of airport security programs. The primary research question included two parts, “To what extent is commercial airport security currently measured and how could it be measured?” The secondary research questions, primarily addressed by the literature review, concerned the applicability of public administration and fire prevention practices to airport security.

Within the limitations outlined in the previous chapter, the Delphi survey indicated airport security is currently measured somewhat crudely. While better metrics would undoubtedly improve public aviation security, implementing the correct performance measures would present numerous challenges. This research identified several management principles that could help meet those challenges: linking organizational mission and goals to performance measures, decentralized participatory management, strategic cost-benefit analysis and budgeting, customer service focus, and anticipatory business continuity planning. While these management concepts are not traditionally employed in the public sector, leading administrators are currently utilizing many. Implementing some form of these management principles could help solve many of the recently reported shortcomings in airport security.

Numerous studies cited in the literature describe how various security programs mandated after 9/11 are hampered by a deficiency of specific objectives, goals, and accepted standards. In *Strategic Planning for Public and Nonprofit Organizations*, John M. Bryson explains how many public organizations fail to accomplish their mission due to a lack of understanding precisely what they are "formally mandated to do." Aviation security providers could benefit from following his four steps to "Clarifying Organizational Mandates and Mission,": 1) listing formal and informal mandates, 2) reviewing the list to determine what is required, forbidden, and allowed, 3) ensuring the organization is aware of these at all times, and 4) frequently evaluating the mandates for needed revisions (Bryson, 2004).

As informal mandates often come from unidentified stakeholders, aviation security providers should also analyze who their key stakeholders are, each one's particular performance criteria, and how well security is meeting those criteria. Once accomplished, these stakeholders should be encouraged to collaborate in creating detailed goals, objectives, and metrics to determine how well these objectives are being achieved. Without this necessary forethought, the organization can easily adopt broad generic security mission and objectives that result in less than full commitment of front line staff and management to their individual responsibilities.

The problem of squandering resources is compounded by the public sector's tendency to enforce rules and line item budgets rigidly. These stringent policies were originally designed to restrain the power of corrupt politicians and inept bureaucrats. Today, however, they tend to prohibit timely adaptation to changing conditions and risks. Furthermore, following rules and staying within budget can be used as a justification for poor decisions, which impedes accountability and conceals incompetence.

In contrast, mission driven organizations facilitate personal responsibility by liberating individuals to increase effectiveness and efficiency through crafting innovative solutions (Osborne & Gaebler, 1992). In the related public safety fields of fire protection standards and building codes, the current trend is to augment prescriptive codes with performance codes, which allows compliance with safety objectives to be demonstrated and encourages engineers, architects, and developers to pioneer new designs and

materials, often cutting costs (Wood, 2000). Nevertheless, original designs do require more expertise, time, and effort to validate because each application is generally unique. Depending on the cost analysis, TSA should pilot the "performance standard" concept in security programs at several pilot airports.

As mission statements are the litmus test tying decisions and actions to values, prior to loosening aviation security standards, each program's mission and objectives must be clearly defined. To quote the Dalai Lama XIV, "Know the rules well, so you can break them effectively" (Good Reads, 2013). Moreover, to increase employee comprehension and retention, these guidelines should be short and easily memorized; some authorities recommend the mission statement should be no more than eight words. An additional benefit is that, when employees understand and retain objectives well, productivity and morale are significantly increased. A positive synergy occurs when team members fully grasp outcome expectations and understand how their individual efforts coordinate to benefit institutional effectiveness (Maxwell 2003). The workforce needs to buy in to the organization's purpose and objectives to adjust to ongoing change in airport security effectively.

This buy-in is more easily achieved through participatory management. When employees are included in the goal and objective development collaboration, they are invested in the outcome (Drucker, 2008). Representatives from the various levels within the security provider organization, as well as members of customer and vender groups affected by the quality of security, should be recruited to create a formal declaration of purpose and related performance standards. Since the staff members executing competency-based policy and programs are in a good position to know what does and does not work, they may also be the best people to help design objective performance measurement tools. The diverse group should not be turned loose to freelance; but should be held accountable with formal direction, based on stakeholder expectations. For instance, guidelines should require objectives be SMART: specific, measurable, ambitious, realistic, and time bound (Poister, 2003). Furthermore, a good beginning might be to consider the security objectives listed by the Transportation Research Board,

of the National Academy of Sciences, Engineering, and Medicine. Their guidelines for transportation security list “deter, detect, deny, and mitigate” as primary objectives (Transportation Research Board of the National Academies, 2006).

In the fire service, these objectives are referred to as prevent, detect, evacuate, and extinguish. For decades, fire safety data has illustrated the effectiveness of a preemptive strategy. If one primary goal of terrorists is to create disruption, chaos, and fear, a good deterrence is the minimization of the resulting consequences of terrorism. Continuity of operation plans are designed to ensure an organization can continue to provide services to its customers as seamlessly as possible, in spite of a crisis; in other words, “minimize the consequences of a crisis.” Security providers should pre-establish lines of succession, alternate sites for specific activities, redundant equipment, and “work around” capabilities as basic elements of a business continuity plan. The existence of these components, or better yet, a Business Continuity Management Certification by the Disaster Recovery Institute (Edwards & Goodrich, 2013), should be monitored by TSA as another quality performance measure of security.

In the private sector, the primary performance indicator is generally considered the profit margin. In the public sector, since profit is rarely a factor, cost-benefit analysis, or quantifying the expense and risk associated with a specific policy or program, is the most closely related measure. In 2009, the Government Accountably Office noted that TSA needed to improve cost-benefit analysis (GAO, 2009) .

The first aviation security financial cost analysis was completed in 1977, when William Landes calculated between 1973 and 1976 that the United States spent $63 million per year enhancing anti-hijacking security, which equates to $238 billion in 2012 dollars, or $34 million per deterred hijacking. The only other cost related research found was when Dr. Qianmei Feng compared the cost effectiveness of two baggage-screening methods 30 years later. She concluded that the increased reliability of using two systems simultaneously more than offset the additional cost. Nevertheless, both these studies were completed within academia, which possibly indicates that while cost benefit analysis should absolutely be an airport security consideration, it may be prudent to partner with research universities for the actual assessments.

Management theory also stresses the importance of listening to and servicing customers. David Osborne and Ted Gaebler in *Reinventing Government* (Osborne & Gaebler, 1992), and Theodore H. Poister in *Measuring Performance in Public and Nonprofit Organizations* (Poister, 2003) recommend allowing operations level staff direct access to customers' feedback. Since perception often determines security effectiveness (Schneier, 2003), customer service surveys can provide relative performance measures, as well as valuable comparative data to improve security. Today, many retailers provide incentives to customers willing to complete short online surveys about specific interactions. Participation rewards customers with a ticket in a gift card raffle in exchange for answering relatively short and simple questions online. These survey instruments are easy and inexpensive to facilitate, due to the prevalence of smart phones, tablets, and wireless Internet service. The retail members of the stakeholder alliance could provide online coupons to entice passengers to take the surveys while waiting for their plane.

Passengers, however, are not the only group served by aviation security providers. Depending on their level and responsibilities, individuals in the security organization could answer to TSA, airport management, multiple airlines, passengers, or freight consignors. John M. Bryson suggests labeling key stakeholders as customers to create employee accountability and emphasize service quality (Bryson, 2004) to entail developing different survey tools for each specific group of stakeholders and customers. Prior to implementation, the cost, time, and effort required for the data collection and analysis should be documented and justified. Once employed, the process should be periodically reviewed, appraised, and refined as necessary.

In his 2013 annual letter, Bill Gates argued that without accurate measurements, the industrial revolution could never have occurred. He points out how picking the right measures, establishing clear and concrete goals, and learning from success is absolutely critical (Gates, 2013). It is imperative that airport administrators recognize how reliable, timely information is necessary to solve today's interconnected and multifaceted airport security problems. If all stakeholders are afforded an opportunity to contribute from their perspective, develop systems to fit their circumstances, and relevant data is analyzed efficiently with a focus on proactive planning, practical solutions can emerge.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX.

A. DELPHI SURVEY ROUND ONE

1.1. "What criteria do you currently use to judge the efficiency and effectiveness of Airport security policies and programs?"

A. Number of passengers waiting 10 minutes or less to be screened. (Checkpoint throughput)

B. TSA Violation History, Security Breaches (At Screening, Passenger Exit Point, and Perimeter), Benchmarking against other airports, and Outside Assessments and Audits.

C. I use the International Civil Aviation Organization Security Audit program, along with a security vulnerability assessment model constructed through personal experience and a variety of vulnerability assessment tools. It also depends on what we're evaluating. GA airports are evaluated differently than commercial service airports.

D. I use a proprietary checklist that examines in detail all aspects of airport/airline/general aviation/support services/cargo operations. Depending upon the size of the operation, going through the checklist, identifying shortfalls, and making recommendations will take anywhere from two days to two weeks.

E. Unfortunately, all too often there has not been an accurate measure of how effective airport security is other than the statement that "there have not been any events or incidents." In the past, the effectiveness has been measured by the number of weapons confiscated at the checkpoint, inspection results, ID compliance, regulatory compliance and the like. None truly represent an effective measure, did we get lucky and nothing happened, or were we tougher than the others and they decided to go somewhere else. The same comparison can be made in measuring illegal immigration and the efforts that have been put into stopping that problem. Are we catching more people, are they finding an alternative method of entry that we cannot measure, or have the numbers of people crossing the border decreased as a result of our efforts. It's impossible to accurately measure a hidden activity.

F. The criterion is to achieve regulatory compliance with least amount of resources expended.

G. Our Airport tracks the following types of information: audits, inspections, access control violations, security incidents. We use this information to 1) focus security audits and inspections on problem areas, 2) plan for capital funding projects to improve security systems (CCTV, video analysis, etc.).

H. Criteria used to judge the efficiency and effectiveness of Airport security policies and programs: Have the appropriate authorities reviewed and approved the specific implementation of the security policies and programs? Have the policies and procedures been reviewed at least annually to ensure they address new requirements and remain relevant? Have exercises been conducted, where appropriate, to ensure procedures are effective? (Such as for: natural disaster alternative procedures or for mass casualty responses.) Have other airport's security programs been reviewed to reveal alternative, perhaps better, ways of security policy and program adherence? Have breaches to security policy and programs been analyzed to assure appropriate procedures are being followed and in response, have policies and programs been adjusted to optimize the system? Have the security policies and programs been tested to ensure they are effective such as: Introduce contraband into the screening process to ensure it is detected

I. Number and Type of incidents and requests for service dispatched, Response times to incidents, Incident assessment time (time to determine if a threat exists after arrival), Number of unauthorized person, or authorized persons without proper credentials, detected within the secure area, Detection rate during daily tests of perimeter/secure area infiltration tests, Cost per boarded passenger to operate security programs (excluding TSA screening), Number of violent and non-violent crimes reported monthly using FBI UCR data, Number of employees and contractors screened and badged monthly

Time to complete screening and badge new employees or contractors, Operational cost impact of security program on terminal tenants and airport contractors, Aircraft delayed due to security events, Have someone walk around a secure area without a badge to test if someone challenges the person.

J. Lack of reported security violations and breaches. Security assessments and covert challenge operations. Spot audits on employee knowledge of security requirements and programs. Lack of regulatory deficiencies discovered by TSA .

1.2. "Which of these do you consider most useful and why?"

A. Checkpoint throughput - this gives an accurate example of customer service.

B. Breaches. They are a "real world" review of the effectiveness to detect, resolve, and recover from a known threat. After-Action Reports serve as the looking glass into procedures and policies so we can determine what works, fails, or needs improvement. They are the most effective means but the least efficient.

C. If I had to give an answer, the ICAO Security Audit would likely be the best.

D. Obviously, the portions of the checklist where shortfalls offer the most likely avenues of approach to commit acts of illegal interference are the most important. But one has to balance that against the known or suspected capabilities of the adversary, and the tactics most likely to be used by them. As an example, if the adversary is known to be likely to favor armed attack against groups of people (i.e., the Lod, Vienna, and Rome attacks of the '80s), we would pay particular attention to security measures that would prevent such attacks, while not ignoring others.

E. I don't believe that there is an accurate measure that can be uniformly applied to measure airport security other than regulatory compliance inspections. Regulations are established and if uniformly enforced and measured, would establish a base-line measurement of an airport's level of security.

F. Regulatory compliance reduces financial risk in the form of fines and having resources in reserve allows the organization to react when specific and credible threats are identified.

G. Tracking of security violations and incidents reflects areas of weakness....for instance a particular airline / tenant may have reoccurring type of violations indicating a lack of training.

H. The most useful criteria to judge the efficiency and effectiveness of Airport security policies and programs is to actually test the system to ensure it responds in the appropriate way.

I. *1.* Number and Type of incidents and requests for service dispatched: Provides key data for assessing the types of staff needed, where policy compliance or physical arrangements are

generating events or reducing events, helps target use of cameras or other solutions to improve response and reduce cost to serve. Frequently identifies areas where security is diverting resources to support other functions, increasing cost to serve and displacing staff from optimal response positions.

2. Incident Response and assessment times: While a reactive measure, this provides insight into staffing (number and location), video assessment tools, prioritization of events, ability to assess and mitigate or escalate. Response is the final line of defense and the one that usually makes the six o'clock news. Given the spread out nature of staff and the need to make quick decisions about departures, a quick assessment to call for support or suspend operations is key to keeping minor incidents from undermining support for the security program, while ensuring that people are kept safe.

3. Detection rates on infiltration tests: Checks policy and training effectiveness, electronic systems effectiveness, roving patrol and tenant awareness, determines areas where improved measures are required (soft spots).

4. Cost per boarded passenger & operational cost to tenants, because this is a basic measure of efficiency, against the business reality of airlines, air cargo and other airport tenants. Cost per passenger when adjusted for regional variance makes for easy comparisons with other airports, which airlines and others seek to justify costs. Operational costs to tenants and contractors is everything from badging and security training to afterhours access delays and is cited as a factor by many contractors and tenants in their costs of doing business at the airport.

J. Security assessments and covert challenge operations – Many facilities and industries have robust and comprehensive security programs, however, the information contained within them is not regularly disseminated to the line personnel. By conducting the assessments and covert operations, it brings this information to the line personnel and ensures that they are receiving the necessary updates.

1.3. "What metrics pertaining to security policy or procedures would you like to see employed? Why?"

A. Passengers waiting 5 minutes or less to be screened. This would speak to the uniqueness of our airport.

B. A catalog and record of all attempts to circumvent security procedures and controls. Access directly to TSA's incident reports that would also allow for data mining and review of events. It would allow the individual airports to spot trends by type, location, or airport size.

C. Metric's for these programs is difficult. Metrics for performance of personnel and equipment is fairly easy, but the challenge is if those performance expectations are placed into an airport or aircraft security program. That makes them binding by regulation, and many operators are hesitant to put performance benchmarks that are not regulatory and that they may not be able to maintain for a myriad of justifiable reasons (budget cuts, lack of promised federal funding, changes in regulatory requirements resulting in operators spending money on systems, methods and procedures that are no longer required, or are required but in a different capacity).

I think for each of those areas where metrics can be developed, they should be. However, there should be flexibility in the system so that operators can take initiatives without worrying about being penalized by the TSA.

D. I'm a little leery of metrics. Too often the ones I've seen depend heavily on numeric scores and this tends to breed a sense of complacency if your score is high. Weighting of various elements of the metrics is always a problem. For instance, do you give more weight (and a lower score) to an airport who has problems maintaining proper perimeter security at points some distance from the terminal, vice not maintaining proper standoff distance for parked cars in the terminal area? Metrics do not and cannot replace the eye of an analyst who not only knows security, but knows the capabilities of any potential adversary, and looks at the system with a view toward what he/she would do to breach the system.

E. A realistic application of threat based risk analysis would be helpful when governments establish security policies and regulations. All too often preventing the doomsday scenario is used as the base-line justification and does not provide a fair comparison.

F. TSA should employ threat assessment and risk analysis for at least 4 categories of airport. Currently, there are two categories of airport to which security directives apply. Certainly, TSA should

make a distinction between BWI and Lincoln, Nebraska in terms of the security risk facing the security managers at those two airports.

G. Since there is no national standard, it may be useful for airports (by category type) to compare metric results w/ other airports and to be able to benchmark solutions. For example, TSA sponsors multiple pilot programs to test for new applications of technology to improve aviation security. Unfortunately, this information is considered SSI and is not shared from one airport to another.

H. The metrics I would like to see employed are related to the empirical testing of the policy or program. Knowing if the system of people and/or equipment can actually detect anomalies enables decision makers to concentrate effort and resources on those areas that have been identified as needing improvement. Each policy and program would have its own set of tests to determine if they are efficient and effective.

I. I would like to see the incident reporting and service request data more standardized and centrally reported across categories of airports (similar to FBI Uniform Crime Reporting) it would be easier to develop best practices and solutions across a range of facilities. Today the role of airport security programs, beyond the TSA mandates, varies greatly by airport even within a category and thus comparisons are difficult. Short of an arrest or investigation by TSA, routine activities that might indicate "probing" across multiple airports would likely not be correlated today unless it was conducted against the screening area, a shared incident reporting infrastructure would make such patterns easier to detect.

J. *1.* Law Enforcement, security and other public safety presence within the Airport environment including the # of personnel and how they are deployed; training; and knowledge of security systems, measures and procedures in place. Why? Deterrence should be the #1 goal of aviation security. Several terrorist incidents have been foiled strictly by police presence in the target location (The Torrance JIS Terrorism Case is an example.) In addition, if the officer is not aware of the requirement, he/she can not fulfill it.

2. Use of technology-based security systems such as hand-held security devices that can read IDs, integrated access control and robust camera systems, central security and public safety

response command centers, etc. Why? This allows public safety and security personnel to monitor security systems in "real time" so that immediate action can be taken. It also reduces human error.

*3***.** Public and employee security awareness programs. Why? Security and law enforcement personnel are a minute part of aviation security in an airport environment. Employees as well as the public user of our airports must support our security efforts. 100,000 pairs of eyes are far greater than the few that are regularly assigned to aviation security efforts. By having a public awareness program, it also instills confidence in our employees and traveling public.

*4***.** Technology based aviation law enforcement and security training systems. Why? One of the biggest complaints in an aviation environment is the fact that training is not on-going. An employee receives their initial airport training and then is generally not subjected to any future formal training. A major concern is the time it takes for employees to go to a central location for this training. By adding electronic kiosks that are accessed via the employees ID and Pin #, the training can be done at any time day or night and the information will be captured for documentation purposes.

*5***.** Audits. Why? If you do not measure the effectiveness of a program, system, measure or procedure, then you cannot actually tell whether it is working or not and/or what improvements and/or efficiencies can be implemented.

B. DELPHI SURVEY ROUND TWO

2.1. According to the first round, there is an apparent desire and willingness to share security performance data. Do you believe a secure web based, professional network, dedicated to airport security information sharing, would be feasible and worth the effort? Why?

A. Yes. This type of network will allow us to quickly "connect the dots." When we determine our threat levels and countermeasures, we have to assess significant bombings, thwarted or discovered plots, special events that are occurring or significant dates. Once that is done we combine this information with current events and we can then see any patterns that are developing as well as devise and implement countermeasures. A secure information network will allow those individuals that develop these countermeasures to have real-time information that is occurring in like disciplines as well as any countermeasures that have been developed that would

be appropriate in a variety of venues. Without this pertinent and time relevant information, the development of countermeasures and security protocols is rendered virtually useless.

B. I do think a website would be a benefit, but if the information contained is voluntary, it would provide only a spotty indication of how airports are doing or how my airport stands in relation to others. To assure evenhandedness and comprehensiveness, I would recommend that the website be hosted by TSA and among other things like a security library and chat rooms on specific subjects, they should publish metrics -- which would need to be established in conjunction with the stakeholders.

C. Yes. It would be a very valuable tool for the sharing of information and experiences from many different areas, regions, perspectives, and agencies. I believe it is now more feasible than in the past, especially with the advent of so many on-line forums that exist today.

D. Shared TSA reports of incidents do help with data-mining. It allows the individual airports to see common events and determine how well they, themselves, are guarded from a similar incident. TSA does have a website for information, though I do not know how much I can discuss since it protected by "SSI."

E. Yes, I absolutely believe we need this. There is a tremendous lack of information sharing in the aviation security industry. There seems to be a lack of trust on the part of the federal government to allow private security practitioners and even local governments like airport operators. When aviation safety became an issue, NASA started the Aviation Safety Reporting System - this allowed the sharing of safety information to go on in a anonymous, non-punitive environment. We need to do the same with aviation security. A good background check will solve most of the security problems and I think most people in the industry would go along with that.

F. Yes, I believe that sharing of security performance data and metrics would be beneficial to all involved. There are a number of different platforms that can be used for this information, although I would suggest that the initiative be undertaken by representative Airport Associations. Wiki's, information sharing platforms such as HSIN could be utilized and existing databases and statistical reporting developed by DOT should be explored as well.

G. The TSA already has a website that ASC's can access but it is under-utilized. The TSA posts incident reports but many that I know do not have time to go through those reports and they're not all that useful. Also, owing to the sensitive nature of some of these issues, I have found that a telephone conversation with a trusted colleague is invaluable.

2.2. Is the International Civil Aviation Organization Security Audit Program a valuable tool? I am not familiar with this program. Why?

A. To my knowledge, it is not readily used in the American aviation environment.

B. I have not worked with the ICAO Security Audit Program.

C. Yes. There is always a need for rules, standards and audits.

D. Not on the individual airport, basis. ICAO's focus is too broad and directed to TSA policy and procedures

E. Yes it is. It's the baseline security elements. Airport and airline operators should however make sure they do other types of audits to cover any gaps in the ICAO program.

F. I cannot comment on the ICAO Security Audit Program since I have not been exposed to it. I have researched it on the web and think that it would form a good starting point for any country specific audit program.

G. I am unfamiliar with the ICAO Security Audit Program but in my work, we used an audit program that was developed locally.

2.3. Considering the concerns and ideas expressed in the survey's first round, what methods would best help determine how to allocate security resources?

A. I believe the best methods to best held determine how to allocate security resources are 1) Analysis of operational losses due to security events; 2) Covert testing and auditing; and 3) Employee awareness of security requirements. Why? With today's economic client, dollars and cents are major concerns of any airport's administration; cost/benefit analysis must accompany every proposal for airport security enhancements. If you can prove that enhanced airport security protocols will cost less that operational losses due to security events, proposals to enhance security will

become more of a business necessity than an aviation security concern. Covert testing allows you to pinpoint areas that require security improvements and provides the necessary data to support your position. And lastly, employee security awareness programs allow you to enlist hundreds, if not thousands in many cases, of additional eyes and ears to assist your security personnel for a minimum amount of funds expended.

B. The best way to allocate security resources is to conduct a risk analysis that would include a vulnerability assessment and a gap analysis to see where resources would be most effectively utilized to increase the level of security.

C. That is a difficult question to answer. It would different things for different areas of the country. It is my opinion that security is a fluid thing, a moving target if you will. While there must be rules and standards, you must also be able to react to an every changing threat. Please note that react may indicate being too late to prevent, but there is only so much anticipation that can be done.

D. An intelligence network that not only relies on airport and aircraft incidents, but relates other events (cyber-attacks, techniques, attempts, etc.) as incidents to be guarded against.

E. This is a big question. I think first there needs to be standard risk assessments - not what "could" occur, but given the circumstances and the threats and threat profiles, there needs to be a national assessment and local assessments. The national assessment should drive a national policy. Local assessments should drive federal funding to allocate the needed resources.

F. I feel that risk based vulnerability assessments are the best method of allocating security resources on a macro level.

G. The TSA is working on a new program to produce a "playbook" where a menu of security measures are outlined and airport operators and FSD's can pick from this menu measures that are tailored to individual airports based on threat assessment. Airports will necessarily employ varying levels of complexity and sophistication based on a threat assessment with local emphasis. I think that's appropriate and I am supportive of this effort.

LIST OF REFERENCES

Alvanou, M. (2008). *Counter terrorism and aviation security.* Retrieved from Research Institute for European and American Studies (RIEAS) website: http://rieas.gr/index.php?option=com_content&task=view&id=363&Itemid=41

Ammons, D. N. (2002) .*Tools for decision making, a practical guide for local government.* Washington, DC: CQ Press.

Aviation sector-specific plan. (2007, May). Retrieved from Department of Homeland Security Library website: http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

Berrick, C. A. (2008). *Testimony before the committee on commerce, science, and transportation, U.S. Senate. transportation security transportation security administration has strengthened planning to guide investments in key aviation and surface transportation security programs, but more work remains* (GAO-08–1024T). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/new.items/d08487t.pdf

Bloomberg new national poll. (2012, March 8–11). Retrieved from media.bloomberg.com website: http://media.bloomberg.com /bb/avfile/rT0NzjIhpqSE

Brearley, H. C. (1916). *Fifty years of a civilizing force: an historical and a critical study of the work of the national board of fire underwriters.* Boston, MA: Stokes.

Brown, B. (2010, June). *Brené Brown: The power of vulnerabitliy*. Retrieved from TED Talks website: http://www.ted.com/talks/lang/en/brene_brown_on _vulnerability.html

Bruegman, R. R. (2012). *Advanced fire administration.* Upper Saddle River, NJ: Pearson Education, Inc.

Bryson, J. M. (2004). *Strategic planning for public and nonprofit organizations.* San Francisco, CA: Jossey-Bass.

Center on Budget and Policy Priorities. (2012, February 12). *States continue to feel recession's impact*. Retrieved from http://www.cbpp.org/files/9–8–08sfp.pdf

Center for Higher Education Policy Studies. (2008). *Welcome to u-map*. Retrieved from U-Map website: http://www.u-map.eu/

Cobb, R. W., & Primo, D. M. (2003). *The plane truth, airline crashes, the media, and transportation policy.* Washington, DC: The Brookings Institute.

Cote, A. E. (2008, October). *History of fire protection engineering*. Retrieved from Fire Protection Engineering website: http://www.fpemag.com/articles/article.asp?i=375

Critical infrastructure and key resources sector-specific plan as input to the national infrastructure protection plan. (2007, May 21). Retrieved from Department of Homeland Security Library website: http://www.dhs.gov/xlibrary/assets/Transportation_Base_Plan_5_21_07.pdf

Department of Homeland Security. (2007, May). *Transportation systems. Critical infrastructure and key resources sector-specific plan as input to the national infrastructure protection plan*. *Transportation systems.* Retrieved from Google website: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CGYQFjAD&url=http%3A%2F%2Fwww.hsdl.org%2F%3Fview%26did%3D474328&ei=HNYsUYvwJpTo8gTdw4HgDA&usg=AFQjCNHhl07FxS1Per0sNzHqZizMXAuxuA

Diamantes, D. (2011). *Principles of fire prevention*. (2nd ed). Cliffton Park, NY: Delmar.

Dillingham, G. L. (1997, March 5). *Testimony before the subcommittee on aviation, committee on commerce, science and transportation, U.S. Senate. Aviation safety and security. Challenges to implementing the recommendations of the White House commission on aviation safety and security* (GAO/T-RCED-97–90). Retrieved from EPIC website: http://epic.org/privacy/faa/gao_aviation_397.pdf

Dillingham, G. R. (2001, September 21). *Testimony before the subcommittee on aviation, committee on transportation and infrastructure, House of Representatives. Aviation security. Weaknesses in airport security and options for assigning screening*. (GAO-01–1165T). Retrieved from The Investigative Project on Terrorism website: http://www.investigativeproject.org/documents/testimony/182.pdf

Drucker, P. F. (2008). *Management revised* . New York, NY: Harper Collins Publishers.

Dunlap, D. W. (2008, March 11). *An airline terminal for a security-wary era*. Retrieved from *New York Times* website: http://www.nytimes.com/2008/03/11/nyregion/11terminal.html?_r=1&oref=slogin

Economist Online. (2010, November 24). *Hands off our junk.* Retrieved from http://www.economist.com/blogs/newsbook/2010/11/airport_security

Edwards, F. L., & Goodrich, D. C. (2013). *Introduction to transportation security.* Boca Raton, FL: Taylor & Francis Group.

Elias, B. (2008, February 25). *Aviation security: Background and policy options for screening and securing air cargo* (Congressional Report No. RL34390). Washington DC: Library of Congress Congressional Research Service. Retrieved from The Naval Postgraduate School Center for Homeland Defense and Security Homeland Security Digital Library website: https://www.hsdl.org/homesec/docs/crs/nps40–030308–03.pdf

Elias, B. (2010). *Airport and aviation security: U.S. policy and strategy in the age of global terrorism.* Boca Raton, FL: Auerbach Publications.

Elrom, S. (2007, October 12). *TSA and aviation security: What is wrong with their concepts and strategy–Part One*. Retrieved from Global Politician website: http://www.globalpolitician.com/articledes.asp?ID=3604&cid=1&sid=107

Feng, Q. (2007). On determining specifications and selections of alternative technologies for airport checked-baggage security screening. *Risk Analysis*, 27.

Gaelber, T., & Osborne, D. (1992). *Reinventing government.* Reading, MA: Addison – Wesley.

GAO. (1999). *Avation security. FAA's actions to study responsibilities and funding for airport security and to certify screening companies* (GAO/RCED-99–53). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/archive/1999/rc99053.pdf

GAO. (2004). *Computer-assisted passenger prescreening system faces significant implementation challenges* (GAO-04–385). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/new.items/d04385.pdf

GAO. (2009). *A national strategy and other actions would strengthen TSA's efforts to secure commercial airport perimeters and access controls* (GAO-09–399). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/new.items/d09399.pdf

GAO. (2010a). *Efforts to validate TSA's passenger screening behavior detection program efforts to validate TSA's passenger screening behavior detection program underway, but opportunities exits to strengthen validation and address operational challenges* (GAO-10–763). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/new.items/d10763.pdf

GAO. (2010b). *Intermodal transportation facilities* (GAO-10–435R). Retrieved from U.S. Government Accountability Office website: http://www.gao.gov/new.items/d10435r.pdf

GAO Highlights.(2011). *Quadrennial homeland security review*. *Enhanced stakeholder consultation and use of risk information could strengthen future reviews*. Retrieved from www.gao.gov/highlights/d11873high.pdf

Gaouette, N. (2007, November 15). *Airport tests reveal major security flaws.* Retrieved from Los Angeles Times website: http://articles.latimes.com/2007 /nov/15/nation/na-screeners15

Gates, B. (2013, January). *2013 annual letter from Bill Gates*. Retrieved from gatesfoundation.org website http://annualletter.gatesfoundation.org/#nav=intro

Good Reads. (2013). *Quotes about rules.* Retrieved from http://www.goodreads.com/quotes/tag/rules

Gordon, S. D. (1914). *Quiet talks aboput the crowned christ.* New York, NY: Fleming H. Revell Co.

Grant, C. C. (1996). *History, the birth of the NFPA.* Retrieved from National Fire Protection Association website: http://www.nfpa.org/itemDetail.asp?categoryID =500&itemID=18020&URL=About NFPA/Overview/History&cook

Great fire of Rome. (n.d.). Retrieved from Associated Publisher website: http://www.associatepublisher.com/e/g/gr/great_fire_of_rome.htm

Gressle, S. S. (2003). *Homeland security act of 2002: Legislative history and pagination key*. Retrieved from www.ndu.edu website: http://www.ndu.edu/library/docs/crs/crs_rl31645_11apr03.pdf

Grimes, R. (2008). *Computer security's dubious future*. Retrieved from Infoworld website: http://www.infoworld.com/article/08/02/22/08OP-security-schneier_2.html

Haimes, Y. Y. (2007, August 3). *Systems-based risk management and analysis*. Retrieved from Naval Postgraduate School website: http://www.nps.edu/Academics/Institutes/Meyer/docs/SI4000/Colloquium_Topic/ Seminar-08–23–2007-Haimes.pdf

Harris, D. H. (2002, Winter). *How to really improve airport security*. Retrieved from Human Factors and Ergonimics Society website: http://www.hfes.org/web/Newsroom/Improve_Airport_Security.pdf

Hatry, H. P., Blair, L. H., Fisk, D. M., Greiner, J. M., Hall, J. R. Jr., & Schaenman, P. S. (1992). *How Effective are your community services? Procedures for measuring their quality.* Washington, DC: ICMA the Urban Institute Press.

Hedgpeth, D. (2008, September 17). *Congress says DHS oversaw $15 billion in failed contracts*. Retrieved from The Washington Post website: http://www.washingtonpost.com/wp-dyn/content/article/2008/09/16/AR2008091603200.html

Hoene, C. W. (2009, December). *City budget shortfalls and responses: Projections for 2010–2012.* Retrieved from The City of El Paos, Texas website: https://www.elpasotexas.gov/muni_clerk/agenda/01–19–10/01191011A.pdf

IATA. (2011, October 10). *The founding of IATA*. Retrieved from http://www.iata.org/about/pages/history.aspx

International Civil Aviation Organization. (2006). Proceedings from International Civil Aviation Conference: *International Civil Aviation Conference, Chicago, Illinois, 1 November to 7 December 1944.* Retrieved from http://www.icao.int/icao/en/chicago_conf/

International Civil Aviation Organization. (2011a). *Annex 17.* Retrieved from http://www2.icao.int/EN/AVSEC/SFP/Pages/Annex17.aspx

International Civil Aviation Organization. (2011b). *History: The beginning*. Retrieved from http://www.paris.icao.int/history/history_1910.htm

Jean, G. (2007, October). Beyond x-ray machines. *National Defense, 92*(647), 28–33.

Kahn, E., & Shoemaker, R. (2006, June 28). *Transportation sector specific plan*. Retrieved from Qdocuments website: http://www.qdocuments.com/Transportation-Sector-Specific-Plan--PPT.html

Kamensky, J. M. (2011, January 6). *GPRA modernization act of 2010 explained: Part 1*. Retrieved from IBM Center for The Business of Government. http://www.businessofgovernment.org/blog/business-government/gpra-modernization-act-2010-explained-part-1

Kelly, D. L. (1999). *Measurement made accessible.* Thousand Oaks, CA: Sage Publications.

Kiuchi, T. (2002). *What we learned in the rainforest, business lessons from nature.* San Francisco, CA: Barrett-Koehler.

Kuepper, G. J. (2004, December). Aviation terrorism—learning from history. *Crisis/Response*, 44–47.

Kunreuthe, H., & Heal, G. (2007). Modeling interdependent risks. *Risk Analysis*, 621–634.

Landes, W. M. (1978). An economic study of U.S. aircraft hijackings, 1960–1976. *Journal of Law and Economics*.

LaPorte, T. R., & Frederickson, H. G. (2002, September). Airport security, high reliability, and the problem of rationality. *Public Administration Review*, *62*(s1), 33–43.

Maxwell, J. (2003). *Developing the leaders around you.* Nashville, TN: Thomas Nelson, Inc.

Maydoney, R. (2005, June 24). *Measuring the performance of a security program, a pinkerton government services white paper*. Retrieved from Aerospace Industries Association website: http://www.aia-aerospace.org/assets/smc_wp-secperform.pdf

Moore, K. C. (1991). *Airport, aircraft, and airline security.* Boston, MA: Butterworth-Heinemann.

Morrison, M. (2010, June 22). *History of SMART objectives*. Retrieved from RAPIDBI website: http://rapidbi.com/history-of-smart-objectives/

National Institute of Standards and Technology. (2010). *NIST special publication 800–37 guide for applying the risk management framework to federal information systems*. Retrieved from http://nistdocs.com/

National strategy for aviation security. (2007, March 26). Retrieved from Department of Homeland Security Library website: http://www.dhs.gov/xlibrary/assets/hspd16_transsystemsecurityplan.pdf

The national strategy for aviation security, sect. II. (2007, March 26). Retrieved from The White House website: http://www.whitehouse.gov/homeland/aviation-security.html

Osborne, D., & Gaebler, T. (1992). *Reienventing government, how the entrepreneurial spirit is transforming the public sector from schoolhouse to statehouse, city hall to pentagon.* Reading, MA: Addison-Wesley Publishing Company.

Parkinson, C. N. (2009, July 10). *Parkins's law*. Retrieved from The Economist website: http://www.economist.com/node/13976732

Peter F. Drucker Literary Trust. (2008). *Management revised.* New York, NY: Harper Collins Publishers.

Peters, G., & Woolley, J. (1970, September 11). *Richard Nixon: Statement announcing a program to deal with airplane hijacking*. Retrieved from http://www.presidency.ucsb.edu/ws/index.php?pid=2659#axzz1bEBMKK1b

Poister, T. H. (2003). *Measuring performance in public and nonprofit organizations.* SanFrancisco, CA: Jossey-Bass.

Preston, N. (2005, February 18). *FAA historical chronology, 1926–1996*. Retrieved from Federal Aviation Administration website: http://www.faa.gov/about/media/b-chron.pdf

Price, J. C., & Forrest, J. S. (2009). *Practical aviation security: Predicting and preventing future threats.* Boston, MA: Elsevier.

Rasbash, D., Ramachandran, G., Kandola, B., Watts, J., & Law, M. (2004). *Evaluation of fire safety.* Chichester, West Sussex, England: John Wiley & Sons Ltd.

Riley, J. (2011, February 28). *Air travel security since 9/11*. Retrieved from Rand Corporation website: http://www.rand.org/content/dam/rand/pubs /corporate_pubs/2011/RAND_CP635.pdf

Rosenbaum, J. (2009, December 2009). *It's time for more security theater*. Retrieved from Firedoglake website: http://my.firedoglake.com/jasonrosenbaum/2009 /12/28/its-time-for-more-security-theater/

Schell, T. L., Chow, B. G., & Grammich, C. (2003). *Designing airports for security: An analysis of proposed changes at LAX*. Retrieved from Rand Corporation website: http://www.rand.org/pubs/issue_papers/IP251/IP251.html

Schneidewind, N. F. (2006). *Homeland security airport security model.* Conference paper. Monterey, CA: Naval Postgraduate School Monterey.

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world.* New York, NY: Copernicus Books.

Shapiro, J. N., & Siegel, D. A. (2010, April 14). *Is this paper dangerous? Balancing secrecy and openness in counterterrorism*. Retrieved from Princeton University website: http://www.princeton.edu/~jns/publications/Is%20This%20Paper %20Dangerous.pdf

Smith, A. (2011, June 6). *Airline industry profits to plunge in 2011*. Retrieved from CNN Money website: http://money.cnn.com/2011/06/06/news/companies/airline_industry/index.htm

Smith, P. (2004). *The essence of leadership*. Retrieved from GovLeaders.org website: http://govleaders.org/essence_of_leadership.htm

Spitzer, D. R. (2007). *Transforming performance measurement.* New York, NY: MACOM.

Sveiby, K.-E., Armstrong, C. (2004, September 4). *Learn to measure to learn! Opening key note address IC congress Helsinki 2 Sept 2004*. Retrieved from sveiby website: http://www.sveiby.com/articles/measuretolearn.pdf

Thomas, A. R. (2008). *Aviation security management.* Westport, CT: Praeger Security International.

Transportation Research Board of the National Academies. (2006). Security Measures for Ferry Systems. *Transportation Security*, *11*, 9.

Wood, K. P. (2000, October). *The effect of performance-based codes and performance-based design on the office of the Illinois state fire marshall.* Retrieved from U.S. Fire Administration website: http://www.usfa.fema.gov/pdf/efop/efo20847.pdf

World: Drama of the desert: The week of the hostages. (1970, September 21). Retrieved from Time Magazine website: http://www.time.com/time/magazine /article/0,9171,942267–2,00.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California